Qualys API V1

User Guide

Version 8.5

July 6, 2015

CONTINUOUS SECURITY

Copyright 2002-2015 by Qualys, Inc. All Rights Reserved.

Qualys, the Qualys logo and QualysGuard are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

Qualys, Inc.
1600 Bridge Parkway
Redwood Shores, CA 94065
1 (650) 801 6100

CONTENTS

Preface

Chapter 1 Welcome

Qualys API v1 Features 10
Processing API Requests 12
Qualys User Account 13
Decoding XML Reports 13
API Conventions 14
API Limits 17

Chapter 2 Vulnerability Scans

About Vulnerability Scanning 22
Scan Functions 25
Scan Request 27
View Running Scans and Maps 35
Cancel a Scan 36
View Scan Report List 38
Retrieve a Saved Scan Report 40
Delete a Saved Scan Report 42
View Scan Target History 44
KnowledgeBase Download 49

Chapter 3 Network Discovery

About Network Discovery 54
Map Functions 58
Map Request — Version 2 60
Map Request — Single Domain 69
View Running Maps and Scans 73
Cancel a Running Map 74
View Map Report List 76
Retrieve a Saved Map Report 78
Delete a Saved Map Report 80

Chapter 4 Account Preferences

Preferences Functions 84
Scheduled Scans and Maps 86
Scan Service Options 100
View Scanner Appliance List 103
View IP List 104
View Domain List 105
View Group List 106

Chapter 5 Asset Management

Asset Management Functions 108
Automatic Host Scan Data 110
Add/Edit Asset IPs 112
View Asset IP List 118
Add/Edit Domains 120
View Asset Domain List 123
Add/Edit Asset Group 124
View Asset Group List 132
Delete Asset Group 133
Search Assets by Attributes 134
Download Asset Data Report 139
Download Asset Range Info Report 143

Chapter 6 Remediation Management

About Remediation Tickets 148
Ticket Functions 150
Ticket Selection Parameters 151
View Ticket List 155
Edit Tickets 158
Delete Tickets 161
View Deleted Ticket List 163
Get Ticket Information 166
Host Functions 169
View Host Information 170
Set Vulnerabilities to Ignore on Hosts 174

Chapter 7 User Management

About User Management 180
User Management Functions 181
Add/Edit Users 182
User Registration Process 193
Accept the Qualys EULA 194
Activate/Deactivate Users 196
View User List 198
Download User Action Log Report 201
User Password Change 204

Appendix A Vulnerability Scan Reports

Scan Results 208
Scan Report List 225
Running Scans and Maps List 228
Scan Target History Output 231
KnowledgeBase Download Output 236

Appendix B Map Reports

Map Report — Version 2 246
Map Report — Single Domain 252
Map Report List 257

Appendix C Preferences Reports

Scheduled Tasks Report 262
Scan Options Report 271
Scanner Appliance List 273
Group List 275

Appendix D Asset Management Reports

Asset IP List 278
Asset Domain List 282
Asset Group List 283
Asset Search Report 287
Asset Range Info Report 294
Asset Data Report 298

Appendix E Remediation Management Reports

Ticket List Output 316
Ticket Edit Output 329
Ticket Delete Output 334
Deleted Ticket List 338
Get Ticket Information Report 341
Get Host Information Report 351
Ignore Vulnerability Output 365

Appendix F User Management Reports

User Output 368
User List Output 370
User Action Log Report 375
Password Change Output 377

Appendix G Error Codes

Index

Preface

Using the Qualys API, third parties can integrate their own applications with Qualys cloud security and compliance solutions using an extensible XML interface. The API functions described in this guide are available to customers with Qualys Vulnerability Management (VM) and Policy Compliance (PC).

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud security and compliance solutions with over 7,700 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100.The Qualys Cloud Platform and integrated suite of solutions help organizations simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications. Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, Accuvant, BT, Cognizant Technology Solutions, Dell SecureWorks, Fujitsu, HCL Comnet, InfoSys, NTT, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA).

For more information, please visit www.qualys.com.

Contact Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/.

CHAPTER 1

Welcome

The Qualys API allows third parties to integrate their own applications with Qualys cloud security and compliance solutions using an extensible XML interface. The API functions described in this guide are available to customers with Qualys Vulnerability Management (VM) and Policy Compliance (PC).

This chapter introduces you to the Qualys API v1. These topics are included:

- Qualys API v1 Features
- Qualys User Account
- Decoding XML Reports
- API Conventions
- API Limits

Additional capabilities are available using the Qualys API v2. For details, please see the Qualys API v2 User Guide.

Qualys API v1 Features

Using the Qualys API v1, partners can access the following Qualys cloud security and compliance features:

- Vulnerability Scans
- Network Discovery
- Account Preferences
- Remediation Management
- User Management

Vulnerability Scans

Qualys vulnerability scans evaluate the security of your network devices and systems and produce reports, with up-to-date information on network security based on the latest vulnerabilities. A vulnerability scan is accomplished by requesting a scan for devices using the scan API functions.

The vulnerability scan functions enable Qualys API users to:

- Scan one or more IP addresses and receive XML scan reports. Each scan request returns a scan report identifying network and systems vulnerabilities found, potential consequences if exploited, and suggested solutions.
- Retrieve a list of scans in progress, and cancel scans in progress.
- Save scan reports on the Qualys server for future use.
- Retrieve and delete saved scan reports.
- View scan history on selected hosts within a certain date range to identify hosts that were scanned and not scanned within a period of time.

Network Discovery

Qualys network discovery produces an inventory of devices detected through a discovery process. Network discovery is accomplished by requesting network maps using the map API functions.

The map functions enable Qualys API users to:

- Request network maps and receive XML map reports. Each map request returns a map report, an inventory of network devices found.
- Retrieve a list of maps in progress, and cancel maps in progress.

- Save map reports on the Qualys server for future use.
- Retrieve and delete saved map reports.

Account Preferences

Preferences are set for each Qualys account, allowing users the ability to customize their experience using the Qualys service. Many preferences are set automatically at account creation time.

The preferences functions enable Qualys API users to:

- Schedule daily, weekly, and monthly scans and maps.
- Set scan service options in the user's default option profile to scan dead hosts, check for load balancers and scan all systems behind them, and set TCP ports to scan.
- List scanner appliances in the user account.

Asset Management

The Qualys API provides many ways to manage assets in the user account. Managers have the ability manage IP addresses and domains (add, edit, list) in the subscription. Users with asset permissions have the ability to manage asset groups, search assets based on asset attributes, and download asset reports based on the latest automatic host scan data.

Remediation Management

Qualys provides fully secure audit trails that track vulnerability status on all scanned IP addresses in the subscription. As follow up audits occur, vulnerability status levels — new, active, fixed, and re-opened — are updated automatically and available for download by API users in various reports, including the asset search report, the asset data report and the asset range info report. The host information report identifies a particular host and its current security status based on the most current automatic host scan data.

Remediation workflow is an optional feature for managing vulnerabilities and their remediation using Qualys' ticketing system. When enabled in the Qualys user interface, new tickets are created automatically based on customer defined policy. As new scan results become available tickets are updated and automatically when previously detected vulnerabilities are verified as fixed. Qualys API users with appropriate account permissions can list tickets, edit tickets, delete tickets and list deleted tickets. The functions provide for simple integration with third-party applications.

User Management

Qualys advocates distributing tasks across functional teams and levels of the organization. Qualys provides a role-based model for assigning user privileges as well as access to IP addresses, domains and scanner appliances. The Qualys API supports adding and editing user accounts, viewing user accounts, downloading user action log reports, and changing user passwords.

Processing API Requests

From the Partner's point of view, the system processes each Qualys API request as illustrated in the figure below.

Figure 1-1. How Qualys API Requests are processed

Step 1 - Receives an HTTPS Request

The partner application establishes a secure HTTP connection (using SSL encryption and "basic" authentication) with the Qualys API Module. For a scan, the HTTP request includes the IP address(es) to be scanned. For a map, the HTTP request includes the domain and/or netblock ranges to be used in the discovery process.

Step 2 - Performs a Qualys Function

The Qualys server performs a variety of functions, including network discovery (maps), network security auditing (scans), adding schedules for maps and scans, retrieving host and ticket information, retrieving account information on IPs, domains, and scanner appliances, and creating new user accounts.

Step 3 - Returns an XML Report

After a function completes, the Qualys server returns a report or status message in XML format.

Qualys User Account

The application must authenticate using Qualys user account credentials (user name and password) as part of HTTP requests made to the Qualys server. For all functions, a Qualys (Front Office) account is required.

If you need assistance with obtaining a Qualys account, please contact your Qualys account representative.

Users with a Qualys user account may access the API to run map and scan functions and view reports. When a subscription has multiple users, all users with any user role (except Contact) can use the Qualys API. Each user's permissions correspond to their assigned user role.

Users may access and view any report including IPs in their account. In the case where a single scan report includes IPs not assigned to the user, the report data does not include the results for the unassigned IPs.

Qualys user accounts enabled with Two Factor Authentication cannot be used with the Qualys API.

Decoding XML Reports

There are a number of ways to parse an XML file. Select the method which is most appropriate for your application and its users.

Qualys publishes DTDs for each report on its Web site. For example, the URL to the scan report can be found at the URL shown below:

```
https://qualysapi.qualys.com/scan-1.dtd
```

The URLs to current report DTDs are included with the function descriptions in this document. There is a generic report returned by a few functions.

Occasionally Qualys updates the report DTDs. It is recommended that you request the most recent DTDs from the Qualys platform to decode your reports. The URLs to the report DTDs are included in this user guide.

Detailed information about each XML report is provided in the appendices at the end of this document. For each XML report a recent report DTD and the report's XML elements and attributes (XPaths) are described in detail.

Some parts of the XML report may contain HTML tags or other special characters (such as accented letters). Therefore, many elements contain CDATA sections, which allow HTML tags to be included in the report. "High" ASCII and other non-printable characters are escaped using question marks.

API Conventions

Before using Qualys API functions, please review the API conventions below.

URL to the Qualys API Server

Qualys maintains multiple Qualys platforms. The Qualys API server URL that you should use for API requests depends on the platform where your account is located.

Account Location	API Server URL
Qualys US Platform 1	https://qualysapi.qualys.com
Qualys US Platform 2	https://qualysapi.qg2.apps.qualys.com
Qualys EU Platform	https://qualysapi.qualys.eu
Qualys Private Cloud Platform	https://qualysapi.<customer_base_url>

The Qualys API documentation and sample code use the API server URL for the Qualys US Platform 1. If your account is located on another platform, please replace this URL with the appropriate server URL for your account.

Authentication

The application must authenticate using Qualys account credentials (user name and password) as part of the HTTP request. The credentials are transmitted using the "Basic Authentication Scheme" over HTTPS.

For more information, see the "Basic Authentication Scheme" section of RFC #2617:

```
http://www.faqs.org/rfcs/rfc2617.html
```

The exact method of implementing authentication will vary according to which programming language is used. See the sample code in Chapter 8, "Sample API Code" for more information.

GET and POST Methods are Supported

Using the Qualys API, you can submit parameters (name=value pairs) using the GET or POST method. Some functions support the GET method only, while others support both the GET and POST methods. There are known limits for the amount of data that can be sent using the GET method. These limits are dependent on the toolkit used. There is no fundamental limit with sending data using the POST method.

All functions support the GET method.

These Network Discovery and Network Scanning functions support the GET and POST methods: map.php, map-2.php, scan.php, scan_report.php, and scheduled_scans.php.

Asset Management functions support the GET and POST methods. Remediation Management functions support the GET and POST methods. User Management functions support the GET and POST methods.

Date Format in API Results

The Qualys API has adopted a date/time format to provide consistency and interoperability of the Qualys API with third-party applications. The date format follows standards published in RFC 3339 and ISO 8601, and applies throughout the Qualys API.

The date format is:

yyyy-mm-dd**T**hh-mm-ss**Z**

This represents a UTC value (GMT time zone).

URL Encoding in API Code

You must URL encode variables when using the Qualys API. This is standard practice for HTTP communications. If your application passes special characters, like the single quote (‘), parentheses, and symbols, they must be URL encoded.

For example, the pound (#) character cannot be used as an input parameter in URLs. If “#” is specified, the Qualys API returns an error. To specify the “#” character in a URL you must enter the encoded value “%23”. The “#” character is considered by browsers and other Internet tools as a separator between the URL and the results page, so whatever follows an un-encoded “#” character is not passed to the Qualys API server and returns an error.

UTF-8 Encoding

The Qualys API uses UTF-8 encoding. The encoding is specified in the XML output header as shown below.

```
<?xml version="1.0" encoding="UTF-8" ?>
```

URL Elements are Case Sensitive

URL elements are case sensitive. The sample URL below will retrieve a previously saved scan report that has the reference code “scan/987659876.19876”. The parameter name “ref” is defined in lower-case characters. This URL will return the specified scan report:

```
https://qualysapi.qualys.com/msp/scan_report.php?
ref=scan/987659876.19876
```

The sample URL below is incorrect and will not return the specified scan report because the parameter name “Ref” appears in mixed-case characters:

```
https://qualysapi.qualys.com/msp/scan_report.php?
Ref=scan/987659876.19876
```

Parameters in URLs

API parameters, as documented in this user guide, should be specified one time for each URL. In the case where the same parameter is specified multiple times in a single URL, the last parameter takes effect and the previous instances are silently ignored.

API Limits

The service enforces limits on the API calls subscription users can make. The limits apply to the use of all APIs, except "session" V2 API (session login/logout).

Important! All API controls are applied on a subscription basis.

Concurrency and Rate Limits

Default settings are provided and these may be customized per subscription by Support.

Concurrency Limit per Subscription (per API). The maximum number of concurrent API call instances allowed within the subscription for each API. Default is 2.

Rate Limit per Subscription (per API). The maximum number of API calls allowed per day (or a customized period, in seconds) within the subscription for each API. The rate limit is defined by the rate limit count and rate limit period. The default rate limit count is 300. The default rate limit period is 86400 seconds (24 hours).

The service checks the concurrency limit and rate limit each time an API request is received. In a case where an API call is received and the service determines a limit has been exceeded, the API call is blocked and an error is returned (the concurrency limit error takes precedence).

Please see the document *Qualys API Limits* for complete information.

API Usage

Your subscription's API usage and quota information is exposed in the HTTP response headers generated by Qualys APIs (all APIs except "session" V2 API).

HTTP Response Headers

The HTTP response headers generated by Qualys APIs are described below.

Note: The HTTP status code "OK" (example: "HTTP/1.1 200 OK") is returned in the header for normal (not blocked) API calls. The HTTP status code "Conflict" (example: "HTTP/1.1 409 Conflict") is returned for API calls that were blocked.

Header	Description
X-RateLimit-Limit	Maximum number of API calls allowed in any given time period of <number-seconds> seconds, where <number-seconds> is the value of X-RateLimit-Window-Sec.
X-RateLimit-Window-Sec	Time period (in seconds) during which up to <number-limit> API calls are allowed, where <number-limit> is the value of X-RateLimit-Limit.

Header	Description
X-RateLimit-Remaining	Number of API calls you can make right now before reaching the rate limit <number-limit> in the last <number-seconds> seconds.
X-RateLimit-ToWait-Sec	The wait period (in seconds) before you can make the next API call without being blocked by the rate limiting rule.
X-Concurrency-Limit-Limit	Number of API calls you are allowed to run concurrently.
X-Concurrency-Limit-Running	Number of API calls that are running right now (including the one identified in the current HTTP response header).

Sample HTTP Response Headers

Sample 1: Normal API call (API call not blocked)

Returned from API call using HTTP authentication.

```
HTTP/1.1 200 OK
Date: Fri, 22 Apr 2011 00:13:18 GMT
Server: qweb
X-RateLimit-Limit: 15
X-RateLimit-Window-Sec: 360
X-Concurrency-Limit-Limit: 3
X-Concurrency-Limit-Running: 1
X-RateLimit-ToWait-Sec: 0
X-RateLimit-Remaining: 4
Transfer-Encoding: chunked
Content-Type: application/xml
```

Sample 2: API Call Blocked (Rate Limit exceeded)

Returned from API call using HTTP authentication.

```
HTTP/1.1 409 Conflict
Date: Fri, 22 Apr 2011 00:13:18 GMT
Server: qweb
X-RateLimit-Limit: 15
X-RateLimit-Window-Sec: 360
X-Concurrency-Limit-Limit: 3
X-Concurrency-Limit-Running: 1
X-RateLimit-ToWait-Sec: 181
X-RateLimit-Remaining: 0
Transfer-Encoding: chunked
Content-Type: application/xml
```

Sample 3: API V2 Call Blocked (Concurrency Limit exceeded)

Returned from API V2 call using API V2 session authentication.

```
HTTP/1.1 409 Conflict
Date: Fri, 22 Apr 2011 00:13:18 GMT
Server: qweb
Expires: Mon, 24 Oct 1970 07:30:00 GMT
Cache-Control: post-check=0,pre-check=0
Pragma: no-cache
X-RateLimit-Limit: 15
X-RateLimit-Window-Sec: 360
X-Concurrency-Limit-Limit: 3
X-Concurrency-Limit-Running: 3
Transfer-Encoding: chunked
Content-Type: application/xml
```

Note: In the case where the concurrency limit has been reached, no information about rate limits will appear in the HTTP headers.

Activity Log within User Interface

The Activity Log within the Qualys user interface shows details about user activities actions taken using the user interface and the API.

To view the Activity Log, log into your Qualys account. Go to VM > Users and click the Activity Log tab. Select Filters > Recent API Calls. Uou'll see the API Processes list showing the API calls subject to the API limits (all APIs except "session" V2 API) made by subscription users and/or updated by the service in the past week.

Tip: You can search the processes list to find API processes. You can search by process state (Queued, Running, Expired, Finished and/or Blocked), by submitted date and by last updated date. You can search for API processes that were blocked due to exceeding the API rate limit and/or the API concurrency limit.

CHAPTER 2

Vulnerability Scans

Qualys performs network security scans on network devices and systems, identifying vulnerabilities and potential vulnerabilities using a powerful scanning engine and a continuously updated Vulnerability KnowledgeBase. At the conclusion of each vulnerability scan, a comprehensive scan report is produced with details about the vulnerabilities and potential vulnerabilities found, and links to recommended fixes.

This chapter describes how to use the Qualys API functions to start and manage vulnerability scans, and access the resulting scan reports:

- About Vulnerability Scanning
- Scan Functions
- Scan Request
- View Running Scans and Maps
- Cancel a Scan
- View Scan Report List
- Retrieve a Saved Scan Report
- Delete a Saved Scan Report
- View Scan Target History
- KnowledgeBase Download

About Vulnerability Scanning

Qualys performs network security scans of your network devices and systems for vulnerabilities. You initiate a network security audit by specifying one or more registered IP addresses to be scanned. The service intelligently runs tests applicable to each target host, including routers, switches, hubs firewalls, Web servers, mail exchangers, servers, workstations, desktop computers, printers and other network appliances.

The scan report includes a comprehensive audit of all vulnerabilities, their severity and potential impact. For each security risk detected, the scan report includes a description of the vulnerability, its severity, potential consequences if exploited, and a recommended solution.

The impact of scans on your network load is minimal because the service samples available bandwidth and then uses a fixed amount of resources. Scan service options allow you to configure the overall performance level, whether dead hosts and/or load balanced hosts will be scanned, and ports to scan. See the "Scan Service Options" section in Chapter 4 for details.

Role of the Option Profile

An option profile is a set of preferences used to process maps and scans. By default, the Qualys API applies the default option profile, as defined in the Qualys user interface, to a new scan request unless another profile is specified.

To create or edit option profiles, use the Qualys user interface. See the Qualys online help for more information.

A selective vulnerability scan may be performed when the option profile is configured to scan user-selected vulnerabilities. When setting up a custom option profile you may wish to include certain vulnerability checks to ensure that certain host information, such as services running, operating system and host names, is available in scan results. If certain checks are not included, then certain vulnerability assessment data will not be available in your scan results and related vulnerability history in other scan reports and views in the user interface. For more information, see "Scan Results and Host Scan Data" in Chapter 5.

Security Audit Process

Security auditing is a dynamic process that involves several main events. The standard behavior for vulnerability scanning events is described below. The service enables this standard behavior in new option profiles, including the "Initial Options (default)" profile that is provided by the service. You can modify this standard behavior by creating or editing an option profile and applying the profile to the scan request.

Host Discovery

The service checks availability of the target hosts. For each host, the service checks whether the host is connected to the network, whether it has been shut down and whether it forbids all Internet connections. The service pings each target host using a combination of ICMP, TCP, and UDP probes based on options configured in the option profile. If these probes trigger at least one response from the host, the host is considered "alive" and the service proceeds to the next event as described in "Port Scanning for Open Ports." If a host is found to be not alive, the audit stops for that host.

The types of probes sent to hosts and the list of ports scanned during host discovery are configurable (on the Additional tab). The service provides "standard" port scanning options, and when these options are enabled TCP and UDP probes are sent to default ports for common services, such as HTTP, HTTPS, FTP, SSH, Telnet, SMTP, DNS, and NetBIOS.

Port Scanning for Open Ports

The service finds open TCP and UDP ports on target hosts. The TCP and UDP ports to be scanned are configurable as scan options in the option profile.

Operating System Detection

The service attempts to identify the operating system installed on target hosts through TCP/IP stack fingerprinting and operating system fingerprinting on redirected ports. The service gathers additional information during the scan process, such as the NetBIOS name and DNS host name when available.

Service Discovery

When TCP or UDP ports are reported as open, the scanning service uses several discovery methods to identify which service is running on the port, and confirms the type of service running to obtain the most accurate data.

Vulnerability Assessment

Each of the previous events results in information gathered for each target host, such as the operating system and version installed, which TCP and UDP ports are open and which services are running on those ports. This information is used to begin vulnerability assessment. The scanning engine runs tests that are applicable to each target host based on the information gathered for the host.

Scanner Appliances

Scanning for security vulnerabilities may be performed using the Qualys External Scanners or Qualys Scanner Appliances. Note that you must use a scanner appliance to scan private use internal IPs on your internal network.

To improve scan speed on large networks, you may choose to use scanner feature to distribute scanning across multiple scanners. See “Scanner Selection for Scans” for more information.

Scan Functions

The vulnerability scan API v1 functions are used to launch and manage scans and these are described in this chapter.

Please Note: We recommend using the scan API v2 functions (endpoint /api/2.0/fo/scan/), instead of the scan API v1 functions, for launching and managing vulnerability scans. The newer scan API v2 provides newer features and added value to users. All the details are explained in the "Qualys API v2 User Guide".

Summary of Scan Functions

The scan API v1 functions are listed below.

Function Name	Description
scan.php	Request a scan for one or more IP addresses that results in producing a scan report. Selective vulnerability scans are supported. URL to the scan report DTD: https://qualysapi.qualys.com/scan-1.dtd
scan_running_list.php	Retrieve a list of running scans and network maps. All scans and maps in progress are listed. URL to the running scans and maps report DTD: https://qualysapi.qualys.com/scan_running_list.dtd
scan_cancel.php	Cancel a scan or map in progress. URL to the generic message DTD: https://qualysapi.qualys.com/generic_return.dtd
scan_report_list.php	Retrieve a list of scan reports in your account. URL to the scans report DTD: https://qualysapi.qualys.com/scan_report_list.dtd
scan_report.php	Retrieve a previously saved scan report. URL to the scan report DTD: https://qualysapi.qualys.com/scan-1.dtd
scan_report_delete.php	Delete a saved scan report. Note that this function may be used to delete a saved map report. This function returns a generic message. URL to the generic message DTD: https://qualysapi.qualys.com/generic_return.dtd

Function Name	Description
scan_target_history.php	Download a report that identifies whether selected hosts were targeted (included in the target) for scans launched in a particular time period. Hosts may be selected by IP address/range or asset group. The XML output identifies IPs targeted and IPs not targeted, based on the request. The output may be restricted to IPs scanned with a certain option profile title, or set of titles. URL to the scan history output DTD: https//qualysapi.qualys.com/scan_target_history_output.dtd
knowledgebase_download.php	Authorized users can download vulnerability data from the Qualys KnowledgeBase, which is constantly updated by Qualys' Research and Development team. Please contact Qualys Support or your sales representative for information. URL to the KnowledgeBase output DTD: https//qualysapi.qualys.com/knowledgebase_download.dtd

Related Functions

Scan-related functions are described in other chapters in this user guide.

Chapter 4, "Account Preferences" describes the schedules function (scheduled_scans.php) which is used to add and remove scan schedules. A scan schedule can be defined to run daily, weekly, monthly or one time only. Once defined, a scan schedule will run automatically.

Chapter 5, "Asset Management" describes the asset management suite. Functionality is provided for managing assets and asset groups based on the permissions set in the user account. Functions allow API users to manage IP addresses and domains in the subscription, manage asset groups, search assets by host attributes, and download asset reports with the most recent host scan data.

Scan Request

scan.php Function

Function Overview

The Vulnerability Scan API (**`/msp/scan.php`** is used to request a Qualys network scan for one or more IP addresses/ranges. At the completion of each scan a scan results report is produced.

Please Note: We recommend using the scan API v2 (/api/2.0/fo/scan/?action=launch), instead of the scan API v1 (/msp/scan.php), for launching vulnerability scans. The newer scan API v2 provides newer features and added value to users. All the details are explained in the *Qualys API v2 User Guide*.

Using the scan API v1 (/msp/scan.php), the scan request parameters specify the scan target (required) and scanner selection (required for scanning private use internal IPs). There are other optional parameters.

Scan Target. The scan target identifies the IPs to be scanned. You may specify a combination of IP addresses, IP address ranges, and asset groups.

To scan target IP addresses using the external scanners, use this URL:

```
https://qualysapi.qualys.com/msp/scan.php?ip={addresses}&
save_report=yes
```

where the **`ip={addresses}`** parameter identifies IPs and/or IP ranges to be scanned, the optional **`save_report=yes`** parameter specifies that the scan report will be saved on the Qualys server.

Use the **`asset_groups={title1,title2...}`** parameter to scan asset groups. See "Target Hosts" for further details.

Scanner Selection. Qualys supports external scanning using its external scanners and internal scanning using Qualys scanner appliances installed inside the corporate network. When a scanner is unspecified for a scan, the external scanners are used. A scanner option must be specified when the task includes internal devices. You may select a scanner appliance name, the "All Scanners in Asset Group" option for scanner parallelization, or the "Default" option for the default scanner in each target asset group.

To scan target asset groups using the scanner parallelization option, use this URL:

```
https://qualysapi.qualys.com/msp/scan.php?
asset_groups={title1,title2...}&scanners_in_ag=1
```

where the **asset_groups={title1,title2...}** parameter identifies the titles of asset groups with IPs to be scanned. See "Scanner Selection for Scans" for further details.

Other parameters. The **scan.php** function applies the default option profile in the user account, unless another profile is specified using the **option={title}** parameter. By default the function scans all vulnerabilities in the Vulnerability KnowledgeBase, however you may limit scanning to select vulnerabilities using the **specific_vulns={Id1,Id2...}** parameter. A scan title may be specified using the **scan_title={title}** parameter.

Hosts Tracked by DNS and/or NetBIOS. To scan hosts tracked by DNS and/or NetBIOS the service must be able to reference the appropriate host names for all target hosts from the host scan data in the user account, otherwise an error is returned. Scan data is part of a host's vulnerability history, which is stored separately from saved scan results. For more information, refer to "Automatic Host Scan Data" in Chapter 5.

Running Scans

While the scan is running, the service uses a "keep alive" mechanism to maintain an open connection to the Qualys server for the duration of the scan. Note that most firewalls terminate a TCP connection if there is no traffic after a minute. To keep the socket alive, the service sends a "< !--keep-alive -->" line every 30 to 40 seconds. These "< ! -- keep-alive -- >" lines appear as comments at the top of the resulting XML scan report, available at the completion of the scan.

At the conclusion of the scan process, the Qualys service returns an XML scan report. This report is not saved on the Qualys server unless the **save_report=yes** parameter is present.

The **scan.php** function cancels a scan in progress if you close the HTTP connection unless **save_report=yes** is set when the scan request is made.

User Permissions

User permissions for the **scan.php** function are described below.

User Role	Permissions
Manager	Scan all IP addresses in subscription.
Unit Manager	Scan IP addresses in user's business unit.
Scanner	Scan IP addresses in user's account.
Reader	No permission to scan IP addresses.

Parameters

The parameters for **scan.php** are described below.

Parameter	Description
scan_title={title}	(Optional) Specifies a title for the scan. The scan title can have a maximum of 2,000 characters. When specified, the scan title appears in the header section of the scan results. When unspecified, the API returns a standard, descriptive title in the header section.
ip={value}	(Optional) Specifies one or more IP addresses and/or ranges to be included in the scan target. Multiple entries must be comma separated. An IP range is specified with a hyphen (for example, 10.10.24.1-10.10.24.20). This parameter and/or **asset_groups** must be specified. The scan target may include a combination of IP addresses and asset groups. See "Target Hosts" below for more information.
asset_groups={title1,title2...}	(Optional) Specifies the titles of asset groups to be included in the scan target. Multiple asset groups must be comma separated. This parameter and/or the **ip** parameter must be specified. The scan target may include a combination of IP addresses and asset groups. See "Target Hosts" below for more information.
exclude_ip_per_scan={value}	(Optional) Used to exclude certain IP addresses/ranges for the scan. One or more IPs/ranges may be specified. Multiple entries are comma separated. An IP range is specified with a hyphen (for example, 10.10.24.1-10.10.24.20).
iscanner_name={name}	(Optional) Specifies the name of the Scanner Appliance for the scan, when the scan target includes internal IP addresses. See "Scanner Selection for Scans" below for more information. One of these parameters may be specified in the same request: **iscanner_name**, **default_scanner**, or **scanners_in_ag**.
default_scanner={**0**|1}	(Optional) Enables the default scanner feature, which is only valid when the scan target consists of asset groups. A valid value is 1 to enable the default scanner, or 0 (the default) to disable it. See "Scanner Selection for Scans" below for more information. One of these parameters may be specified in the same request: **iscanner_name**, **default_scanner**, or **scanners_in_ag**.

Parameter	Description
scanners_in_ag={**0**|1}	(Optional) Enables the scanner parallelization feature, which is only valid when the scan target consists of asset groups. A valid value is 1 to enable scanner parallelization, or 0 (the default) to disable it. See "Scanner Selection for Scans" below for more information.
	One of these parameters may be specified in the same request: **iscanner_name**, **default_scanner**, or **scanners_in_ag**.
specific_vulns={Id1,Id2,Id3...}	(Optional) Specifies a selective vulnerability scan. When set, the service scans your target IPs for the one or more vulnerabilities you specify. Enter a comma-separated list of Qualys IDs for the vulnerabilities you wish to scan. A maximum of 250 vulnerabilities may be selected for a single scan. If specified, it's recommended that you include certain QIDs to ensure host information is available in your scan results and other reports. For more information, see "Scan Results and Host Scan Data" in Chapter 5.
option={title}	(Optional) Specifies the title of an option profile to be applied to the scan. The profile title must be defined in the user account, and it can have a maximum of 64 characters. If unspecified, the default option profile in the user account is applied. Note that custom option profiles can be added only using the Qualys user interface. You can specify the title of a custom option profile with selected vulnerabilities (a subset of the QIDs in the KnowledgeBase). It's recommended that you include certain QIDs to ensure host information is available in your scan results and other reports. For more information, see "Scan Results and Host Scan Data" in Chapter 5.

Parameter	Description
save_report={**no** | yes}	(Optional) Used to save the scan report on the Qualys server for later use. A valid value is "yes" to save the scan report, or "no" (the default) to not save the report. When set to "yes", you can close the HTTP connection when the scan is in progress, without cancelling the scan. When the scan completes the resulting scan report is saved on the Qualys server, and a scan summary email notification is sent (if this option is enabled in your user account). Saved scan reports can be retrieved using the **scan_report_list.php** and **scan_report.php** functions.
runtime_http_header={value}	Set a custom value in order to drop defenses (such as logging, IPs, etc) when an authorized scan is being run. The value you enter will be used in the "Qualys-Scan:" header that will be set for many CGI and web application fingerprinting checks. Some discovery and web server fingerprinting checks will not use this header.

Target Hosts

The host target identifies IP addresses to be scanned and reported on. A host target may include a combination of user-entered IPs, in the form of individual IPs and/or IP ranges, as well as asset groups that contain IPs.

IP Addresses and Ranges

A host target may include IP addresses and/or ranges.

Using the **scan.php** function, user-entered IPs are specified in the **ip={addresses}** parameter. Using the **scheduled_scans.php** function, these IPs are specified in the **scan_target={addresses}** parameter. IP addresses may be entered using the formats described below:

Multiple IPs. Multiple IP addresses must be comma separated like this:

```
123.123.123.1,123.123.123.4,123.123.123.5
```

IP Ranges. An IP address range specifies a start and end IP address separated by a dash (-) like this:

```
123.123.123.1-123.123.123.8
```

IPs and Ranges. A combination of IPs and IP ranges may be specified. Multiple entries must be comma separated like this:

```
123.123.123.1-123.123.123.5,194.90.90.3,194.90.90.9
```

Asset Groups

The **asset_groups={title1,title2...}** parameter identifies titles of one or more asset groups with IPs to be scanned and reported on. Only asset group titles in the user account may be specified.

Multiple Asset Group Titles. Multiple titles must be comma separated, as shown below:

```
Corporate,Finance,Customer+Service
```

Asset Group Title "All". The asset group title "All" includes all IPs in the user account. This asset group title may be specified for most API functions as indicated in the individual function descriptions in this user guide.

Scanner Selection for Scans

For each scan — an on demand scan or a scheduled scan — a scanner is applied to the task. External scanning at the network perimeter is supported by the Qualys external scanners, and internal scanning of private use internal IPs is supported using Qualys Scanner Appliances. Private use internal IPs must be scanned using scanner appliances, which are installed inside the corporate network.

When a scanner is unspecified for a scan task, the Qualys External Scanners are used. A scanner option must be selected when the scan target includes internal devices. You may select a scanner appliance name, the All Scanners in Asset Group option for scanner parallelization, or the Default option for the default scanner in each target asset group.

External Scanners

The external scanners at the Qualys Security Operations Center (SOC) can be used for scanning external IPs, devices on your network perimeter that can be "seen" from the Internet. The external scanners are used by default when a scanner appliance name is unspecified and the default scanner feature is disabled.

Scanner Appliance Name

A scanner appliance can be used for scanning IPs on the internal network. Use the **iscanner_name** parameter to specify the scanner appliance name for a scan request. If the scan target is the "All" group and the user account has private use internal IPs, a scanner appliance name is the only valid scanner option.

Scanner Parallelization

The scanner parallelization feature, for internal scanning, increases scan speed making a scan up to 4 times faster, depending on the size of the network, while maintaining the scan accuracy. Such an increase in speed allows scanning all ports when required. This feature is available for both on demand and scheduled scans.

The scanner parallelization feature allows you to distribute a scan task to multiple scanner appliances, when the scan target includes asset groups. Use the **scanners_in_ag** parameter to enable scanner parallelization for a scan request. When this feature is enabled, the scan task is distributed to multiple scanner appliances in parallel. The first 5 scanner appliances added to each target asset group make up the pool of scanners used to scan the group's IP addresses. At the completion of the scan, the service compiles a single report with scan results.

During scan processing, if a scanner appliance is not available for some reason, perhaps because it is offline, the service automatically distributes the scan task to another appliance in the same scanner appliance pool for the asset group.

A scan task may be distributed across scanner appliances that have the same software versions (vulnerability signatures and scanner) at the time of the scan. If one of the scanner appliances in the pool has a software version that does not match the other scanner appliances, then it will not be used. If some scanner appliances have identical software versions and others do not, then appliances with the most matching versions are used, regardless of whether the software is the most current. For example, if 3 appliances have the same software version and the other 2 appliances have a different version, then the 3 appliances with the same software version are used.

Default Scanner

The default scanner feature allows you to distribute a scan task to the default scanner in each target asset group. Use the **default_scanner** parameter to enable the default scanner for a scan request. When this feature is enabled, the default scanner as defined in each target asset group is used for scanning the asset group's IP addresses. When multiple asset groups are scanned, the scan request is distributed to the various scanners (scanner appliances and/or extenal scanners) and the service compiles a single report with scan results.

Examples

To scan the IP address "123.123.123.7", receive a scan report, and save the scan report on the Qualys server, specify this URL:

```
https://qualysapi.qualys.com/msp/scan.php?ip=123.123.123.7&
save_report=yes
```

To scan more than one IP address and receive a scan report, the IP addresses must be comma separated as shown in the example URL below:

```
https://qualysapi.qualys.com/msp/scan.php?
ip=1.2.3.4-1.2.3.9,1.2.3.20
```

To scan the IP address “123.123.123.7” for the Microsoft MFC Could Allow Remote Code Execution (MS07-012) (Qualys ID 90381) and the Microsoft VBScript Remote Code Execution Vulnerability (KB981169) - Zero Day (Qualys ID 90587) using the scanner appliance “Milan”, specify this URL:

```
https://qualysapi.qualys.com/msp/scan.php?ip=123.123.123.7&
specific_vulns=90381,90587&iscanner_name=Milan&scan_title=
IP+123.123.123.7&save_report=yes
```

To scan the asset groups “Corporate” and “New York” using the default scanner, the option profile “Profile A”, and the scan title “My Network Security Report”, specify this URL:

```
https://qualysapi.qualys.com/msp/scan.php?asset_groups=
Corporate,New+York&default_scanner=1&option=Profile+A&
scan_title=My+Network+Security+Report&save_report=yes
```

To scan the asset groups “Unix Servers” and “Finance” using the scanner parallelization feature, the option profile “Initial Options” and the scan title “Scan+with+Scanner+Parallelization”, specify this URL:

```
https://qualysapi.qualys.com/msp/scan.php?asset_groups=
Unix+Servers,Finance&scanners_in_ag=1&option=Initial+Options&
scan_title=Scan+with+Scanner+Parallelization&save_report=yes
```

XML Report

The DTD for the XML scan report returned by the **`scan.php`** function can be found at the following URL:

```
https://qualysapi.qualys.com/scan-1.dtd
```

Appendix A provides information about the XML report generated by the **`scan.php`** function, including a recent DTD and XPath listing.

View Running Scans and Maps

scan_running_list.php Function

The Scan Running List API (/msp/**scan_running_list.php** is used to retrieve a list of scans and network maps that are currently running in XML format. To retrieve a list of running scans and maps, use the following URL:

```
https://qualysapi.qualys.com/msp/scan_running_list.php
```

For each scan and map task, the XML output includes a reference code and properties. The reference code can be used to cancel a running scan or map using the **scan_cancel.php** function.

User permissions for the **scan_running_list.php** function are described below.

User Role	Permissions
Manager	View all running maps/scans in subscription.
Unit Manager	View running maps/scans in user's business unit, including their own tasks and tasks run by other users in the same business unit.
Scanner	View running scans/maps in user's account.
Reader	No permission to view running maps/scans.

Please Note: We recommend using the scan list API v2 (/api/2.0/fo/scan/?action=list), instead of the running scan list API v1 (/msp/scan_running_list.php). The newer scan API v2 provides newer features and added value to customers. All the details are explained in the *Qualys API V2 User Guide*.

XML Report

The DTD for the XML running scans and maps list report returned by the **scan_running_list.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/scan_running_list.dtd
```

Appendix A provides information about the XML report generated by the **scan_running_list.php** function, including a recent DTD and XPath listing.

Cancel a Scan

scan_cancel.php Function

The Scan Cancel API (**/msp/scan_cancel.php**) is used to cancel a scan (or map) in progress. It's not possible to cancel a scan when it has the status "Loading". To cancel a scan, use the following URL:

```
https://qualysapi.qualys.com/msp/scan_cancel.php?
  ref={referenceCode}
```

where the **ref={referenceCode}** parameter specifies the scan reference for the scan to be cancelled.

User permissions for the **scan_cancel.php** function are described below.

User Role	Permissions
Manager	Cancel any scan in progress in subscription.
Unit Manager	Cancel any scan in progress in user's business unit, including user's own scans and scans run by other users in the same business unit.
Scanner	Cancel any scan in progress in user's account.
Reader	No permission to cancel scans.

Please Note: We recommend using the scan cancel API v2 (/api/2.0/fo/scan/?action=cancel), instead of the scan cancel API v1 (/msp/scan_cancel.php). The newer scan API v2 provides newer features and added value to customers. All the details are explained in the *Qualys API V2 User Guide*.

Parameters

The one parameter for **scan_cancel.php** is described below.

Parameter	Description
ref={value}	(Required) Specifies the scan reference for the scan in progress . A scan reference starts with "scan/". To find the appropriate reference, use the **scan_running_list.php** function or the V2 scan API function (see the *Qualys API V2 User Guide*).

Example

To cancel a scan in progress with the reference code "scan/987659876.19876", use the following URL:

```
https://qualysapi.qualys.com/msp/scan_cancel.php?
  ref=scan/987659876.19876
```

XML Success Message

When you cancel a scan, the **scan_cancel.php** returns an XML success message like this:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE GENERIC_RETURN SYSTEM
"https://qualysapi.qualys.com/generic_return.dtd">
<GENERIC_RETURN>
  <API name="scan_cancel" username="joe" at="2005-03-
08T16:17:42Z" />
   <RETURN status="SUCCESS">
     The scan will be cancelled ASAP.
  </RETURN>
</GENERIC_RETURN>
```

The DTD for the message returned by the **scan_cancel.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/generic_return.dtd
```

View Scan Report List

scan_report_list.php Function

The Scan Report List API (**/msp/scan_report_list.php**) is used to retrieve a list of saved scan reports in XML format. To list scan reports, use the following URL:

```
https://qualysapi.qualys.com/msp/scan_report_list.php
```

User permissions for the **scan_report_list.php** function are described below.

User Role	Permissions
Manager	View all saved scan reports in subscription.
Unit Managers	View saved scan reports for IP addresses in user's business unit.
Scanner	View saved scan reports for IP addresses in user's account.
Reader	View saved scan reports for IP addresses in user's account.

Please Note: We recommend using the scan list API v2 (/api/2.0/fo/scan/?action=list), instead of the scan report list API v1 (/msp/scan_report_list.php). The newer scan API v2 provides newer features and added value to customers. All the details are explained in the *Qualys API V2 User Guide*.

Parameters

The parameters for **scan_report_list.php** are described below.

Parameter	Description
last={**no** | yes}	(Optional) Used to retrieve information only about the last saved scan report. A valid value is "yes" to retrieve the last saved report or "no" (the default) to retrieve all scan reports.
target={address}	(Optional) Used to retrieve all saved scan reports for a target IP address.
since_datetime={value}	(Optional) Used to filter the report list, including only saved scan reports for scans launched since a certain date/time. If time is not specified, the list output includes reports for scans launched anytime during the entire day. The date/time is specified in this format (UTC/GMT): YYYY-MM-DD[THH:MM:SSZ] For example: "2008-12-11" or "2008-12-11T23:30:00Z"

If you include both **target={address}** and **last=yes**, you will receive information about the last saved scan that included the target IP address.

Examples

To receive a list of saved scan reports for the target IP address "123.123.123.4", specify this URL:

```
https://qualysapi.qualys.com/msp/scan_report_list.php?
  target=123.123.123.4
```

To receive information about the last saved scan, specify this URL:

```
https://qualysapi.qualys.com/msp/scan_report_list.php?
  last=yes
```

To receive information about the last saved scan that included the target IP address "123.123.123.4", specify this URL:

```
https://qualysapi.qualys.com/msp/scan_report_list.php?
  last=yes&target=123.123.123.4
```

To receive a list of saved scan reports for scans launched since January 10, 2010 (anytime during the day), specify this URL:

```
https://qualysapi.qualys.com/msp/scan_report_list.php?
  since_datetime=2010-01-10
```

XML Report

The DTD for the XML scan report list report returned by the **scan_report_list.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/scan_report_list.dtd
```

Appendix A provides information about the XML generated by the **scan_report_list.php** function, including a recent DTD and XPath listing.

Retrieve a Saved Scan Report

scan_report.php Function

The Scan Report API (**/msp/scan_report.php**) is used to retrieve a saved scan report. Complete scan results are available only when the scan status is "Finished". If the scan status is other than "Finished" some scan results may be available. To retrieve a saved scan report, use the following URL:

```
https://qualysapi.qualys.com/msp/scan_report.php?
  ref={referenceCode}
```

where the **ref={referenceCode}** parameter specifies the scan report to be retrieved.

User permissions for the **scan_report.php** function are described below.

User Role	Permissions
Manager	View saved scan report in subscription.
Unit Managers	View saved scan report for IP addresses in user's business unit.
Scanner	View saved scan report for IP addresses in user's account.
Reader	View saved scan report for IP addresses in user's account.

Please Note: We recommend using the scan API v2 (/api/2.0/fo/scan/?action=fetch), instead of the scan report API v1 (/msp/scan_report.php). The newer scan API v2 provides newer features and added value to customers. All the details are explained in the *Qualys API V2 User Guide*.

Parameters

The parameters for **scan_report.php** are described below.

Parameter	Description
ref={value}	(Required) Specifies the scan reference for the scan to be retrieved. A scan reference starts with "scan/". To find the appropriate reference, use the **scan_report_list.php** function or the V2 scan API function (see the *Qualys API V2 User Guide*).
target={value}	(Optional) Used to specify that the scan report will include sections that match one or more specified IP addresses. Multiple IPs/ranges may be specified. See "Target Hosts" for information.

Examples

To retrieve a saved scan report with the reference code "scan/987659876.19876", use the following URL:

```
https://qualysapi.qualys.com/msp/scan_report.php?
  ref=scan/987659876.19876
```

To retrieve a saved scan report with the reference code "scan/987659876.19876", including sections that match the target IPs "123.123.123.4" and "123.123.123.7" only, use the following URL:

```
https://qualysapi.qualys.com/msp/scan_report.php?
  ref=scan/987659876.19876&target=123.123.123.4,123.123.123.7
```

XML Report

The reports returned by the **scan_report.php** and **scan.php** functions have the same DTD. The DTD for the XML report returned by these functions can be found at the following URL:

```
https://qualysapi.qualys.com/scan-1.dtd
```

Typically a scan report returned from the **scan_report.php** function is returned quicker than a report returned from the **scan.php** function because the **scan_report.php** function returns scan report data for a scan that has already been performed.

Appendix A provides information about the XML scan report generated by the **scan.php** and **scan_report.php** functions, including a recent DTD and XPath listing.

Delete a Saved Scan Report

scan_report_delete.php Function

The Scan Report Delete API (**/msp/scan_report_delete.php**) is used to delete a saved scan report, when the scan status is "Finished". To delete a saved scan report, use the following URL:

```
https://qualysapi.qualys.com/msp/scan_report_delete.php?
  ref={referenceCode}
```

where the **ref={referenceCode}** parameter specifies the scan report to be deleted.

User permissions for the **scan_report_delete.php** function are described below.

User Role	Permissions
Manager	Delete saved scan reports in the subscription.
Unit Manager	Delete saved scan reports for IPs in user's business unit, including user's own scans and scans run by other users in the same business unit.
Scanner	Delete saved scan reports in user's account.
Reader	No permission to delete scan reports.

Please Note: We recommend using the scan API v2 (/api/2.0/fo/scan/?action=delete), instead of the scan report delete API v1 (/msp/scan_report_delete.php). The newer scan API v2 provides newer features and added value to customers. All the details are explained in the *Qualys API V2 User Guide*.

Parameters

The one parameter for **scan_report_delete.php** is described below.

Parameter	Description
ref={value}	(Required) Specifies the scan reference for the scan to be deleted. A scan reference starts with "scan/". To find the appropriate reference, use the **scan_report_list.php** function or the V2 scan API function (see the *Qualys API V2 User Guide*).

XML Success Message

The **scan_report_delete.php** returns an XML success message like this:

```
<?xml version="1.0" encoding="UTF-8" ?>
```

```
<!DOCTYPE GENERIC_RETURN SYSTEM
"https://qualysapi.qualys.com/generic_return.dtd">
<GENERIC_RETURN>
   <API name="scan_report_delete.php" username="joe"
at="2002-03-27T14:29:08Z" />
<RETURN status="SUCCESS">
    The operation was successfully completed.
</RETURN>
</GENERIC_RETURN>
```

The DTD for the message returned by the **scan_report_delete.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/generic_return.dtd
```

View Scan Target History

scan_target_history.php Function

The Scan Target History API (**/msp/scan_target_history.php**) identifies whether selected hosts were targeted (included in the target) for scans launched during a certain time period. Hosts may be selected by IP address/range or asset group. The XML output may be restricted IPs scanned with a certain option profile title, or set of titles.

The scan target history output includes an IP Targeted List and/or an IP Not Targeted List based on the request. The IP Targeted List includes IPs on which scan task(s) were launched, regardless of the scan outcome (completed, canceled or aborted). A targeted IP may or may not have been actually scanned as in the case when the service does not complete the scan because the host was "not alive". The IP Not Targeted List includes IPs on which scan task(s) were not launched.

An optional input parameter allows you to include detailed history about scanned hosts in the IP Targeted List. When specified, detailed history for each scan on each host is provided, including the date/time when the scan was launched, the scan reference code, the option profile used, the scan job status (at the time of the request), and whether the scan results were deleted.

User permissions for the **scan_target_history.php** function are described below.

User Role	Permissions
Manager	View scan history for scans on all IP addresses in subscription.
Unit Manager	View scan history for scans on IP addresses in user's business unit.
Scanner	View scan history for scans on IP addresses in user's account.
Reader	View scan history for scans on IP addresses in user's account.

Parameters

The parameters for **scan_target_history.php** are described below.

Host Selection Parameters

The **scan_target_history.php** request must specify target hosts. The **ips** parameter is used to specify IP addresses and/or ranges. The **asset_group** parameter is used to specify a single asset group. One of these parameters is required. These parameters are mutually exclusive, and cannot be specified together in the same request.

Parameter	Description
ips={addresses}	(Optional) Specifies one or more IP addresses and/or ranges to be included in the scan history report. Multiple entries are comma separated.
	This parameter or the **asset_group** parameter must be specified. You cannot specify this parameter and the **asset_group** parameter in the same request.
asset_group={title}	(Optional) Specifies one asset group title to be included in the scan history report. The title "All" may be specified to include all IP addresses in the user account.
	This parameter or the **ips** parameter must be specified. You cannot specify this parameter and the **ips** parameter in the same request.

IP Targeted/Not Targeted List Parameters

The **scan_target_history.php** request must specify whether the output will include the IP targeted list and/or the IP not targeted list using the parameters: **ip_targeted_list** and **ip_not_targeted_list**.

Parameter	Description
ip_targeted_list={**0**|1}	(Optional) Specifies whether the IP targeted list will be included in the output. When unspecified, the parameter is set to 0 and the IP targeted list is not included. When this parameter is specified and set to 1, the list is included.
	This parameter or the **ip_not_targeted_list** parameter must be specified and set to 1.
ip_not_targeted_list={**0**|1}	(Optional) Specifies whether the IP not targeted list will be included in the output. When unspecified, the parameter is set to 0 and the IP not targeted list is not included. When this parameter is specified and set to 1, the list is included.
	This parameter or the **ip_targeted_list** parameter must be specified and set to 1.

Date Range Parameters

The request must specify a date range for retrieving scan data. Scans launched within this period will be retrieved and included in your report. The **date_from** parameter (required) and the **date_to** parameter (optional) are used to specify this date range.

The date range specified in a single request may include a maximum of 12 months. If a request identifies a longer period an error message is returned.

The date range parameters for **scan_target_hostory.php** are described below.

Parameter	Description
date_from={value}	(Required) Specifies the start date/time of the time window for retrieving scan data. Scans launched on or after this date/time will be included in the report. The start date/time is specified in UTC/GMT format. See "Date/Time Format" below. The date range specified by this parameter and the **date_to** parameter (optional) may include a maximum of 12 months.
date_to={value}	(Optional) Specifies the end date/time of the time window for retrieving scan data. Scans launched on or before this date/time will be included in the report. If not specified, the end date/time is set to the date/time when the request is made. The end date/time is specified in UTC/GMT format. See "Date/Time Format" below. The date range specified by this parameter and the **date_from** parameter may include a maximum of 12 months.

Date/Time Format

The start and end date/time is specified in this format (UTC/GMT):

```
YYYY-MM-DD[THH:MM:SSZ]
```

where date (YYYY-MM-DD) is required and time is optional.

For example you can specify: "2006-01-01" or "2006-05-25T23:12:00Z".

The date element is required and the time element is optional. If time is not specified, the following values are set by the application automatically.

Range	Parameter	Default Time (when not supplied)
Start Date	date_from	T00:00:00Z
End Date	date_to	T23:59:59Z

Additional Parameters

The additional parameters (optional) for **`scan_target_history.php`** are below.

Parameter	Description
option_profile_title={prefix:text}	(Optional) Specifies a filter to restrict the output to IPs targeted with a certain option profile title or a set of option profile titles in the user's subscription. A filter is entered in this format: option_profile_title=prefix:text A valid prefix is: begin, match, contain, or end. The text string may include a maximum of 64 characters (ascii). Note: When this parameter is properly specified, the output does not include deleted scans. Do not specify this parameter if you wish to retrieve information on deleted scans.
detailed_history={**0**|1}	(Optional) Specifies whether the output will include detailed history for IPs targeted. If you set **`detailed_history=1`**, detailed history data is included for IPs targeted. When specified, detailed history for each scan on each host is provided, including the date/time when the scan was launched, the scan reference code, the option profile used, the scan job status (at the time of the request), the scan title, and whether the scan results were deleted.

Examples

To view scan history from June 1, 2009 on all IP addresses in your account with the IP targeted list and the IP not targeted list, specify this URL:

```
https://qualysapi.qualys.com/msp/scan_target_history.php?asset_
group=All&date_from=2009-06-01&ip_targeted_list=1&
ip_not_targeted_list=1
```

To view scan history from August 4, 2009 on the asset group "New York" and an option profile title starting with "SANS20", specify this URL:

```
https://qualysapi.qualys.com/msp/scan_target_history.php?asset_
group=New+York&date_from=2009-08-04&ip_targeted_list=1&option_
profile_title=begin:SANS20
```

To view scan history from March 1, 2009 to June 30, 2009 on the IP range 10.10.10.1-10.10.10.100 and include scan history details, specify this URL:

```
https://qualysapi.qualys.com/msp/scan_target_history.php?ips=10
.10.10.1-10.10.10.100&date_from=2009-03-01&date_to=2009-06-30&
ip_targeted_list=1&detailed_history=1
```

XML Report

The DTD for the XML scan target history output report returned by the **`scan_history.php`** function can be found at the following URL:

```
https://qualysapi.qualys.com/scan_target_history_output.dtd
```

Appendix A provides information about the XML generated by the **`scan_target_history.php`** function, including a recent DTD and XPath listing.

KnowledgeBase Download

Function Overview

The Qualys Cloud Platform includes a KnowledgeBase with the industry's largest number vulnerability signatures. The KnowledgeBase is continuously updated by Qualys' Research and Development team. Qualys is fully dedicated to providing the most accurate security audits in the industry. Each day new and updated signatures are tested in Qualys' own vulnerability labs and then published, making them available to Qualys customers.

The KnowledgeBase Download API (**`/msp/knowledgebase_download.php`**) allows authorized Qualys users to download contents of the Qualys KnowledgeBase to benefit from a comprehensive solution that is always up to date. Please contact Qualys Support or your sales representative if you would like to use this API.

Express Lite: This API is available to Express Lite users.

Please Note: We recommend using the KnowledgeBase API v2 (/api/2.0/fo/knowledge_base/vuln/?action=list), instead of the KnowledgeBase download API v1 (/msp/knowledgebase_download.php). The newer API v2 provides newer features and added value to customers. All the details are explained in the *Qualys API V2 User Guide*.

knowledgebase_download.php Function

The **`knowledgebase_download.php`** function allows authorized Qualys users to download the vulnerability data for the entire Qualys KnowledgeBase (all vulnerabilities) or for a single Qualys vulnerability (QID).

To download the data for the entire KnowledgeBase, use this URL:

```
https://<qualysapi.qualys.com>/msp/knowledgebase_download.php
```

where <qualysapi.qualys.com> is the Qualys server URL where your Qualys account is located.

After making a **`knowledgebase_download.php`** request, a KnowledgeBase download XML report is returned with vulnerability data in English.

The vulnerability data returned from a **`knowledgebase_download.php`** request corresponds to the data in your user account. Customizations to vulnerabilities are downloaded, such as custom severity levels and descriptions for threat, impact, and solution. Also user-defined OVAL vulnerabilities are downloaded.

User permissions for the **knowledgebase_download.php** function are described below. Note: Your subscription must be granted permission to run this function. Please contact Qualys Support or your sales representative to receive this authorization.

User Role	Permissions
Manager, Unit Manager, Scanner, Reader	Download vulnerability data from the KnowledgeBase.
Auditor	No permission to download vulnerability data from the KnowledgeBase.

Parameters

The parameters for **knowledgebase_downlaod.php** are described below.

Parameter	Description
vuln_id={value}	(Optional) Specify the QID number for a vulnerability in the KnowledgeBase to return vulnerability data for. When specified, only vulnerability data for the selected QID will appear in the XML output.
show_cvss_submetrics={**0**|1}	(Optional) Specify **1** to show CVSS submetrics for vulnerabilities in the XML output when the CVSS scoring feature is enabled in the user account. When unspecified, CVSS submetrics are not shown in the XML output.
show_pci_flag={**0**|1}	(Optional) Specify **1** to show the PCI flag for vulnerabilities in the XML output. Also the reasons for passing or failing PCI compliance will be shown (when the CVSS scoring feature is enabled for your account). The PCI flag identifies whether the vulnerability must be fixed to pass PCI compliance. When unspecified, the PCI flag and reasons are not shown.
is_patchable={**0**|1}	(Optional) For each vulnerability in the XML output, the service indicates whether a patch is available to fix the issue. Specify **1** to show only vulnerabilities which have patches in the XML output. Specify **0** to show only vulnerabilities which do not have patches in the XML output. When unspecified, all vulnerabilities are included.

Examples

To download the data for a single Qualys vulnerability (QID), use this URL:

```
https://qualysapi.qualys.com/msp/knowledgebase_download.php?
vuln_id=38461
```

To download the data for all Qualys vulnerabilities (QIDs) including CVSS submetrics when the CVSS scoring feature is enabled in your account, use this URL:

```
https://qualysapi.qualys.com/msp/knowledgebase_download.php?
show_cvss_submetrics=1
```

To download the data for a single Qualys vulnerability (QID) including CVSS submetrics (when the CVSS scoring feature is enabled in your account) and the PCI flag, use this URL:

```
https://qualysapi.qualys.com/msp/knowledgebase_download.php?
vuln_id=38461&show_cvss_submetrics=1&show_pci_flag=1
```

XML Report

The DTD for the KnowledgeBase output report returned by the **knowledgebase_download.php** function can be found at the following URL:

```
https://<qualysapi.qualys.com>/knowledgebase_download.dtd
```

where <qualysapi.qualys.com> is the Qualys server URL where your Qualys account is located.

Appendix A provides information about the XML generated by the **knowledgebase_download.php** function, including a recent DTD and XPath listing.

CHAPTER 3

Network Discovery

Qualys network discovery produces an inventory of all network devices on your network. Qualys accurately characterizes devices including: access points to the network, machine names, IP addresses, operating systems, and discovered services such as HTTP, SMTP, and Telnet.

This chapter describes how to use the Qualys API functions to start and manage network maps and the resulting map reports:

- About Network Discovery
- Map Functions
- Map Request — Version 2
- Map Request — Single Domain
- View Running Maps and Scans
- Cancel a Running Map
- View Map Report List
- Retrieve a Saved Map Report
- Delete a Saved Map Report

About Network Discovery

The Qualys map is a network discovery tool that finds network devices for one or more domains, and produces an inventory of the devices found. The map provides you with a topology of your network elements — on the perimeter or within the internal network. The discovery process can detect devices and services running without authorization, placed by a non-authorized user. It also finds weaknesses due to DNS server and other network mis-configurations. Networks are continually evolving and changes in firewall rules or DNS setups may allow intruders to find more information than they should.

For each map request, Qualys generates a network map report in XML format. The map report includes the following information about the devices found:

- Operating systems
- Access points to the network
- IP addresses and machine names
- Methods used to discover devices
- Discovered services, such as HTTP, SMTP, and Telnet

Discovering Your Network Perimeter

A map request produces a map of visible devices on your network perimeter. These are devices that can be "seen" from the Internet. It provides you with an outside-in perspective of your network elements. The scope of the discovery includes the devices found for a domain through the domain's DNS (Domain Name Server), plus the devices between those devices and the Internet. For this reason, the map report may include more devices than those identified by a domain.

Discovering Your Internal Network

If you use a Qualys Scanner Appliance, which is installed inside the corporate network, the map service produces a map of visible devices on your internal network. All devices that can be "seen" from the Intranet by the appliance are included in the map report. The scope of the network discovery includes the devices found for a domain through the internal DNS in your network plus the devices between those devices and the Scanner Appliance. For this reason, the map report may include more devices than those identified by a domain.

The Role of the Option Profile

An option profile is a set of preferences used to process maps and scans. By default, the Qualys API applies the default option profile, as defined in the Qualys user interface, to a new map request unless another profile is specified.

A new Qualys account has a pre-defined, default option profile called "Initial Options." You have the ability to edit this profile and create custom profiles in the Qualys user interface. See the Qualys online help for more information.

The Discovery Process

The discovery process begins by using each target domain's DNS to find as many hosts within that domain as possible. Then information is gathered about each identified host.

The following methods Qualys uses to find hosts within a specified domain:

- The service identifies the Name Server (NS), and then sends a request to list all the hosts managed by the NS. Note that this request is not always allowed and may be forbidden by the administrator.
- Using a proprietary list of roughly 100 common names, such as www or ftp, to form a list of Fully Qualified Domain Names (FQDN), the service queries the NS to find the IP address assigned to each FQDN.
- The service sequentially checks IP addresses provided as netblocks in the domain specification, if any (see "Using Domains with Netblocks" below).

After hosts in the domain are identified, Qualys determines whether hosts are alive and gathers information about the hosts, such as information about the operating system and routers detected on each host. Operating system detection is mainly based on TCP/IP stack fingerprinting. Multiple information gathering methods may be employed. Note that the precise methods used relate to the option profile configuration (see the next section "Discovery Events").

Discovery Events

Network discovery for each domain is a dynamic process that involves two main events: host discovery and basic information gathering. The standard behavior for these events is described below. Qualys enables this standard behavior in new option profiles, including the "Initial Options" profile. You can modify this standard behavior by creating or editing an option profile and applying the profile to the map.

Host Discovery

Qualys gathers data from public records to identify hosts in each domain using various methods including Whois lookups, DNS zone transfer, and DNS brute force. The service then checks availability of the hosts in the target domain. For each host, the service checks whether the host is connected to the network, whether it has been shut down and whether it forbids all Internet connections.

The service pings each target host using a combination of TCP, UDP, and ICMP probes based on the option profile configuration. If these probes trigger at least one response from the host, the host is considered "alive" and the service proceeds to the next event as described in "Basic Information Gathering on Hosts." If a host is found to be not alive, discovery stops for that host.

The types of probes sent to hosts and the list of ports scanned during host discovery are configurable in the option profile. With the standard options enabled, the service sends probes to TCP, UDP, and ICMP ports for common services, such as HTTP, HTTPS, FTP, SSH, Telnet, SMTP, DNS, and NetBIOS. For information about the profile configuration, including the ports scanned, view the option profile in the Qualys user interface.

Basic Information Gathering on Hosts

Qualys attempts to identify the operating system installed on each host, and scans standard TCP ports to determine which ports are open. Note that by performing basic information gathering, additional scan tests are launched, which may result in the detection of additional devices, such as routers.

The type of hosts scanned (all hosts, registered hosts, netblock hosts, or none) and the list of ports scanned for open port detection and operating system detection are configurable as map options (on the Map tab). With the standard options are enabled, the service scans 13 standard TCP ports for common services. For information about profile configuration, including the ports scanned, view the option profile in the Qualys user interface.

Using Domains with Netblocks

Domains may include one or more network IP address ranges called *netblocks*. Netblocks are included in a domain specification to expand the scope of the discovery process beyond the domain. Domain specifications are defined for your Qualys account at account creation time and/or later using the Qualys user interface.

When you launch a map for a domain with netblocks, Qualys collects information about these devices: a) devices discovered in the domain, b) devices discovered in the netblocks, and c) devices discovered between “a” and “b” and the Internet (or the Scanner Appliance when producing a map for your internal network). Using netblocks in this way enables the user to be certain that specific IP addresses are included in the resulting map report.

The domain named “none” identifies a netblock without a domain name. There can be only one “none” domain in your account. This is useful for scanning an internal network using Scanner Appliances because an internal network may not have a domain name defined, or an internal DNS server may not be present. When you launch a map for the network perimeter using the “none” domain with netblocks, Qualys discovers devices between the IP addresses defined in the netblock and the Intranet. When you launch a map for the internal network using the “none” domain with netblocks, the service discovers devices between the netblock IP addresses and the Scanner Appliance.

Scanner Appliances

Network discovery may be performed using the Qualys External Scanners or Qualys Scanner Appliances. Note that you must use a scanner appliance to map domains with private use internal IPs on your internal network. This includes domains for which Qualys will discover internal IPs and domains with netblocks that have internal IPs.

You may choose to use the default scanner feature to distribute mapping across multiple scanners when the map target has asset groups. See “Scanner Selection for Maps” for more information.

Map Functions

The map functions are used to perform the following: request network maps for domains and receive map reports, retrieve a list of maps in progress, cancel maps in progress, save map reports on the Qualys server for future use, retrieve and delete saved map reports. Map-related functions assist with managing map tasks.

Summary of Map Functions

The map functions are listed below. For each map function a summary description is provided. Detailed descriptions and examples for all functions are provided in the following sections.

Function Name	Description
map-2.php	Request a network map for one or more domains that produces an inventory of network devices. The default scanner may be used to distribute mapping of target asset groups across multiple scanners. This function provides enhancements to the map.php function. URL to the map report DTD: https://qualysapi.qualys.com/map-2.dtd
map.php	Request a network map for a single domain that produces an inventory of network devices. URL to the map report DTD: https://qualysapi.qualys.com/map.dtd
scan_running_list.php	Retrieve a list of running maps and scans. All scans and maps in progress are listed. URL to the running scans and maps report DTD: https://qualysapi.qualys.com/scan_running_list.dtd
scan_cancel.php	Cancel a map or scan in progress. URL to the map report DTD: https://qualysapi.qualys.com/map.dtd
map_report_list.php	Retrieve a list of map reports in your account. URL to the map report list DTD: https://qualysapi.qualys.com/map_report_list.dtd

Function Name	Description
map_report.php	Retrieve a previously saved map report for a particular domain. URL to the map report DTD: https://qualysapi.qualys.com/map.dtd
scan_report_delete.php	Delete a saved map report for a particular domain. Note that this function may be used to delete a saved scan report. This function returns a generic message. URL to the generic message DTD: https://qualysapi.qualys.com/generic_return.dtd

Related Functions

Map-related functions are described in other chapters in this user guide.

Chapter 4, "Account Preferences" describes the schedules function (scheduled_scans.php) which is used to add and remove map schedules. A map schedule can be defined to run daily, weekly, monthly or one time only. Once defined, a map schedule will run automatically.

Chapter 5, "Asset Management" describes the asset management suite. Functionality is provided for managing assets and asset groups based on the permissions set in the user account. Functions allow API users to manage IP addresses and domains in the subscription, manage asset groups, search assets by host attributes, and download asset reports with the most recent host scan data.

Map Request — Version 2

map-2.php Function

Function Overview

The Network Map API (**/msp/map-2.php** is used to request a Qualys network map for one or more domains. The map target may include asset groups and the default scanner option may be enabled for distributed mapping across multiple scanner appliances. This function provides enhancements to the map.php function.

Express Lite: This API is available to Express Lite users.

The map request parameters specify the map target (required) and scanner selection (required for scanning private use internal IPs). There are other optional parameters.

Map Target. The map target identifies the domains to be mapped. You may specify both user-entered domain names and asset groups.

To map a target domain using the external scanners, use this URL:

```
https://qualysapi.qualys.com/msp/map-2.php?domain={target}
```

where the **domain={target}** parameter specifies the domains for which a network map will be produced. This parameter may be specified with a netblock. See "Target Domains" for further details.

Use the **asset_groups={title1,title2...}** parameter to scan asset groups. See "Target Domains" for further details.

Scanner Selection. Qualys supports external domain mapping using its external scanners and internal domain mapping using Qualys Scanner Appliances. When a scanner is unspecified, external scanners are used. A scanner option must be specified when the target domain includes internal devices. You may select a scanner appliance name or the Default option for the default scanner in each target asset group.

To map domains in asset groups using the default scanner, use this URL:

```
https://qualy-
sapi.qualys.com/msp/map-2.php?asset_groups={title1,title2...}&d
efault_scanner=1
```

where the **asset_groups={title1,title2...}** parameter identifies titles of asset groups with domains to be mapped. See "Scanner Selection for Maps" for further details.

Other parameters. The **map-2.php** function applies the default option profile in the user account, unless another profile is specified using the **option={title}** parameter. A map title may be specified using the **map_title={title}** parameter.

Running Maps

While the map is running, the service uses a "keep alive" mechanism to maintain an open connection to the Qualys server for the duration of map processing. Note that most firewalls terminate a TCP connection if there is no traffic after a minute. To keep the socket alive, the service sends a "< !--keep-alive -->" line every 30 to 40 seconds. These "< ! -- keep-alive -- >" lines appear as comments at the top of the resulting XML map report, available at the completion of the map. See Appendix B to view a sample map report containing these lines.

At the conclusion of the network discovery process, the Qualys service returns an XML map report. This report is not saved on the Qualys server unless the **`save_report=yes`** parameter is present.

The **`map-2.php`** function cancels a map in progress if you close the HTTP connection unless **`save_report=yes`** is set when the map request is made.

User Permissions

User permissions for the **`map-2.php`** function are described below.

User Role	Permissions
Manager	Map all domains in subscription.
Unit Manager	Map domains in user's business unit.
Scanner	Map domains in user's account.
Reader	No permission to map any domains.

Parameters

The parameters for **`map-2.php`** are described below.

Parameter	Description
map_title={title}	(Optional) Specifies a title for the map. The map title can have a maximum of 2,000 characters. When specified, the map title appears in the header section of the map results. When unspecified, the API returns a standard, descriptive title in the header section.
domain={target}	(Optional) Specifies one or more domains to be included in the map target. For each domain, include the domain name only; do not enter "www." at the start of the domain name. Netblocks may be specified with each domain name to extend the scope of the map. Multiple domains must be comma separated. This parameter and/or **`asset_groups`** must be specified. The map target may include both domain names and asset groups. See "Target Domains" below for more information.
asset_groups={title1,title2...}	(Optional) Specifies the titles of asset groups to be included in the map target. Multiple asset groups must be comma separated. This parameter and/or the **`domain`** parameter must be specified. The map target may include both a domain name and asset groups. See "Target Domains" below for more information.
iscanner_name={name}	(Optional) Specifies the name of the Scanner Appliance for the map, when the map target has private use internal IPs. See "Scanner Selection for Maps" below for more information. Using Express Lite, Internal Scanning must be enabled in your account.
	One of these parameters may be specified in the same map request: **`iscanner_name`** or **`default scanner`**.
default_scanner=1	(Optional) Enables the default scanner feature, which is only valid when the map target consists of asset groups. A valid value is 1 to enable the default scanner, or 0 (the default) to disable it. See "Scanner Selection for Maps" below for more information. Using Express Lite, Internal Scanning must be enabled in your account.
	One of these parameters may be specified in the same map request: **`iscanner_name`** or **`default scanner`**.

Parameter	Description
option={title}	(Optional) Specifies the title of an option profile to be applied to the map. The profile title must be defined in the user account, and it can have a maximum of 64 characters. If unspecified, the default option profile in the user account is applied. Note that custom option profiles can be defined only using the Qualys user interface.
save_report=yes	(Optional) Saves a map report for each target domain on the Qualys server for later use. A valid value is "yes" to save a map report for each target domain, or "no" (the default) to not save the report. If set to "yes", you can close the HTTP connection when the map is in progress, without cancelling the map. When the map completes the resulting map report is saved on the Qualys server, and a map summary email notification is sent (if this option is enabled in your user account). Saved map reports can be retrieved using the **`map_report_list.php`** and **`map_report.php`** functions.

Target Domains

The map target defined for the map request identifies the domains to be mapped. A map target may include both user-entered domains and asset groups that contain domains.

Domains

A map task may include multiple domains when the **`map-2.php`** function for an on demand map or the s**`cheduled_scans.php`** function is used for a scheduled map. When using the **`map.php`** function for an on demand map, the map target may include a single domain.

Using the **`map-2.php`** function, user-entered domains are specified in the **`domain={target}`** parameter. Using the **`scheduled_scans.php`** function for a scheduled map, domains are specified in the **`scan_target={target}`** parameter. Using the **`map.php`** function, a single domain may be specified in the **`domain={target}`** parameter.

Domain Formats

A domain can be identified as follows: 1) a domain name, 2) a domain name with netblocks (one or more IPs and/or IP ranges), or 3) the special "none" domain with netblocks. The "none" domain allows you to run multiple maps and map reports on different network segments.

The domain specification is "domain:netblocks", where the domain element is the domain name (or fully qualified domain name) and each netblock may identify a single IP address or IP range.

When running a map, netblocks may be included with a domain specification to expand the scope of the discovery process beyond the domain. See "The Discovery Process" earlier in this chapter for information about network discovery and how netblocks are used in the network discovery process.

Domains may be specified as follows:

Domain	Example
Domain Name	mydomain.com
Multiple Domain Names	mydomain1.com,mydomain2.com
Domain Name with Netblocks	
Single IP	mydomain.com:64.41.134.60
IP Range	mydomain.com:10.10.10.1-10.10.10.100
IP Range and Single IP	mydomain.com:10.10.10.1-10.10.10.100;64.41.134.60
User-specified IP	none:64.41.134.61

Domain	Example
User-specified IPs	none:64.41.134.61;64.41.134.65
User-specified IPs/Ranges	none:64.41.134.59-64.41.134.61;10.10.10.10

When specifying a target domain, use the following syntax:

- Separate the domain name and the netblocks by a colon (:).
- For a netblock with an IP range, use a dash (-) to separate the first and last IP.
- For multiple netblocks, use the semi-colon (;) to separate the netblocks.

Domain Definitions

The user-entered target domains you supply for the map target override the domain definition in your Qualys account. Let's say that your account has this domain:

```
mail.mymail.com:192.168.0.1-192.168.0.254
```

If you specify "domain=mail.mymail.com", then the discovery process involves host detection and information gathering for the target domain and the netblock.

If you specify "domain=mail.mymail.com:192.1680.1-192.168.0.100", then the discovery process involves host detection and information gathering for "mail.mymail.com" and the netblock "192.1680.1-192.168.0.100". In this case, discovery includes fewer IPs than those defined for the domain in the account.

It's possible to specify the domain name with two netblocks, fragments of the netblock defined in the account. For the "mail.mymail.com" domain, you can specify:

```
domain=mail.mymail.com:192.168.0.1-192.168.0.10;192.168.0.20-
192.168.0.100
```

The netblock in a map request overrides the netblock defined in the user account.

Asset Groups

The **`asset_groups={title1,title2...}`** parameter identifies titles of one or more asset groups with domains for the map request. Only asset group titles in the user account may be specified.

Scanner Selection for Maps

For each map — a map request or a scheduled map — you must select a scanner to apply to the task. External scanning at the network perimeter is supported by the Qualys External Scanners, and internal scanning of private use internal IPs is supported using Qualys Scanner Appliances.

Domains with private use internal IPs must be mapped using scanner appliances, which are installed inside the corporate network. Domains for which the service discovers internal IPs and domains specified with internal IPs in a netblock must be mapped using scanner appliances.

Select one of these scanner options for each map. To map a domain with external devices, select Qualys External Scanners. To map a domain with internal devices, select a Scanner Appliance name or the Default Scanner option for the default scanner in each target asset group.

When a scanner is unspecified for a map task, the Qualys External Scanners are used. A scanner option must be selected when the map target includes internal devices. You may select a Scanner Appliance name or the Default Scanner option for the default scanner in each target asset group.

External Scanners

The external scanners at the Qualys Security Operations Center (SOC) can be used for mapping domains with external IPs, devices on the network perimeter that can be "seen" from the Internet. The external scanners are used by default when a scanner appliance name is unspecified and the default scanner is disabled.

Scanner Appliance Name

A scanner appliance can be used for mapping domains on the internal network. Use the **`iscanner_name`** parameter to specify the scanner appliance name for a map request. If the map target is the "All" group and the user account has domains with private use internal IPs, a scanner appliance name is the only valid scanner option.

Default Scanner

The default scanner feature allows you to distribute a map task to the default scanner in each target asset group. Use the **`default_scanner`** parameter to enable the default scanner for a map request. When this feature is enabled, the default scanner as defined in each target asset group is used for mapping the asset group's domains. When multiple asset groups are mapped, the map request is distributed to the various scanners (scanner appliances and/or external scanners) and the service compiles a single report with map results.

Examples

To request a map of the domain "www.mycompany.com" using the external scanners and to receive a map report, use this URL:

```
https://qualysapi.qualys.com/msp/map-2.php?domain=mycompany.com
```

To request a map of the domain "www.mycompany.com" using the external scanners, and to receive a map report and save it on the Qualys server, use this URL:

```
https://qualysapi.qualys.com/msp/map-2.php?domain=mycompany.com
&save_report=yes
```

To request a map of the domain "www.mycompany.com" using the option profile "My Profile" and the scanner appliance "London" and to receive a map report, use this URL:

```
https://qualysapi.qualys.com/msp/map-2.php?domain=mycompany.com
&option=My+Profile&iscanner_name=London
```

To request a map for the following domain/netblock pair using the scanner appliance "Hong Kong":

```
mycompany.com:192.168.0.1-192.168.0.254
```

use this URL:

```
https://qualysapi.qualys.com/msp/map-2.php?domain=mycompany.com:19
2.168.0.1-192.168.0.254&iscanner_name=Hong+Kong
```

To request a map for this domain/netblock pair using the scanner appliance "San Francisco":

```
none:192.168.0.1-192.168.0.254
```

use this URL:

```
https://qualysapi.qualys.com/msp/map-2.php?domain=none:192.168.0.1
-192.168.0.254&iscanner_name=San+Franscisco
```

To request a map of the domains in asset groups “Corporate”, “Finance”, and “Operations” using the default scanner and the option profile “My Profile”, to receive a map report and it on the Qualys server, use this URL:

```
https://qualysapi.qualys.com/msp/map-2.php?asset_groups=Corporate,
Finance,Operations&default_scanner=1&option=My+Profile&save_report
=yes
```

XML Report

The DTD for the XML map report returned by the **`map-2.php`** function can be found at the following URL:

```
https://qualysapi.qualys.com/map-2.dtd
```

Appendix B provides information about the XML report generated by the **`map-2.php`** function, including a recent DTD and XPath listing.

For a map request with multiple domains, the XML map report returned by the **`map-2.php`** function includes all domains that were successfully discovered. Note that when you view the map results for this request using the **`map_report.php`** function or the Qualys user interface, each map report includes map results for one domain. Also, if the map summary notification is enabled in your account, there is a separate notification for each target domain.

Map Request — Single Domain

map.php Function

Function Overview

The **map.php** function is used to request a Qualys network map for a domain, initiating the network discovery process. To request a network map, use the following URL:

```
https://qualysapi.qualys.com/msp/map.php?domain={target}
```

where the **domain={target}** parameter specifies the domain for which a network map will be produced. This parameter is required and may be specified with a netblock. See "Target Domain — Single Domain" for more information.

Only one domain can be specified for each map request, as shown in the example below:

```
https://qualysapi.qualys.com/msp/map.php?domain=mydomain.com
```

The target domain you specify must be defined in your Qualys account. You may add domains to your account using the Qualys user interface. For information, refer to the Qualys online help.

The **map.php** function applies the default option profile in the user account, unless another profile is specified using the **option={title}** parameter. The external scanner is used, unless a scanner appliance is specified using the **iscanner_name={name}** parameter.

Running Maps

While the map is running, the service uses a "keep alive" mechanism to maintain an open connection to the Qualys server for the duration of map processing. Note that most firewalls terminate a TCP connection if there is no traffic after a minute. To keep the socket alive, the service sends a "< !--keep-alive -->" line every 30 to 40 seconds. These "< ! -- keep-alive -- >" lines appear as comments at the top of the resulting XML map report, available at the completion of the map.

At the conclusion of the network discovery process, the Qualys service returns an XML map report. This report is not saved on the Qualys server unless the **save_report=yes** parameter is present.

The **map.php** function cancels a map in progress if you close the HTTP connection unless **save_report=yes** is set when the map request is made.

User Permissions

User permissions for the **map.php** function are described below.

User Role	Permissions
Manager	Map any domain in subscription.
Unit Manager	Map domain in user's business unit.
Scanner	Map domain in user's account.
Reader	No permission to map any domains.

Parameters

The parameters for **map.php** are described below.

Parameter	Description
map_title={title}	(Optional) Specifies a title for the map. The map title can have a maximum of 2,000 characters. When specified, the map title appears in the header section of the map results. When unspecified, the API returns a standard, descriptive title in the header section.
domain={target}	(Required) Specifies the target domain. Include the domain name only; do not enter "www." at the start of the domain name. Netblocks may be specified with a domain name. See "Target Domain — Single Domain" below for more information.
iscanner_name={name}	(Optional) Specifies the name of the scanner appliance to be used for the map. If the map target has private use internal IPs, you must specify this parameter. See "Scanner Selection for Maps — Single Domain" below for more information.

Parameter	Description
option={title}	(Optional) Specifies the title of an option profile to be applied to the map. The profile title must be defined in the user account, and it can have a maximum of 64 characters. If unspecified, the default option profile in the user account is applied. Note that custom option profiles can be defined only in the Qualys user interface.
save_report=yes	(Optional) Saves the map report on the Qualys server for later use. When specified, a map summary email notification is sent to users who have this option enabled in their user accounts. A valid value is "yes" to save the map report, or "no" (the default) to not save the report. If set, you can close the HTTP connection when the map is in progress, without cancelling the map. In this case, the map continues and the resulting map report is saved on the Qualys server. Saved map reports can be accessed using the **`map_report_list.php`** and **`map_report.php`** functions.

Target Domain — Single Domain

Use the **`domain={target}`** parameter specifies the target domain for a map request. The target domain specified in this parameter must be defined in the user account.

Netblocks may be included with a domain specification to expand the scope of the discovery process beyond the domain. See "The Discovery Process" earlier in this chapter for more information.

One of these formats may be specified as the target domain: Domain only, Domain with netblocks and Netblock only. For more information, see "Domain Formats" and "Domain Definitions" earlier in this chapter.

Scanner Selection for Maps — Single Domain

For each map request using the **`map.php`** function, you must select a scanner to apply to the task. External scanning at the network perimeter is supported by the external scanner and enabled by default, and internal scanning of private use internal IPs is supported using a Qualys Scanner Appliance.

A domain with private use internal IPs must be mapped using a scanner appliance. A domain for which the service discovers internal IPs and a domain which includes a netblock with internal IPs must be mapped using a scanner appliance.

To use a scanner appliance, specify the scanner appliance name using the **`iscanner_name={name}`** parameter. If unspecified, the external scanner is used.

Examples

To request a map of the domain "www.mycompany.com" using the scanner appliance "My Scanner" and the default option profile, and to receive a map report, use this URL:

```
https://qualysapi.qualys.com/msp/map.php?domain=mycompany.com&iscanner_name=My+Scanner
```

To request a map of the domain "www.mycompany.com" using the appliance "My Scanner" and the option profile "My Profile" and to receive a map report, use this URL:

```
https://qualysapi.qualys.com/msp/map.php?domain=mycompany.com&iscanner_name=My+Scanner&option=My+Profile
```

To request a map of the domain "www.mycompany.com" using the scanner appliance "Tiger" and the default option profile and to receive a map report and save the map report on the Qualys server, use this URL:

```
https://qualysapi.qualys.com/msp/map.php?domain=mycompany.com&iscanner_name=Tiger&save_report=yes
```

To request a map using the scanner appliance "Tiger" for this domain/netblock pair:

```
mycompany.com:192.168.0.1-192.168.0.254
```

use this URL:

```
https://qualysapi.qualys.com/msp/map.php?domain=mycompany.com:192.168.0.1-192.168.0.254&iscanner_name=Tiger
```

To request a map using the scanner appliance "Giraffe" for this domain/netblock pair:

```
none:192.168.0.1-192.168.0.254
```

use this URL:

```
https://qualysapi.qualys.com/msp/map.php?domain=none:192.168.0.1-192.168.0.254&iscanner_name=Giraffe
```

XML Report

The DTD for the XML map report returned by the **`map.php`** function can be found at the following URL:

```
https://qualysapi.qualys.com/map.dtd
```

Appendix B provides information about the XML report generated by the **`map.php`** function, including a recent DTD and XPath listing.

View Running Maps and Scans

scan_running_list.php Function

The **scan_running_list.php** function is used to retrieve a list of maps and scans that are currently running. To retrieve a list of running maps and scans, use the following URL:

```
https://qualysapi.qualys.com/msp/scan_running_list.php
```

The **scan_running_list.php** function returns a list of currently running scans and network maps in XML format. For each scan and map, this information is provided: a reference code, a start date/time, the target IP addresses (for a scan), the target domain (for a map), the number of hosts already scanned, and a flag indicating whether the scan or map is a scheduled task. The reference code can be used to cancel a running scan or map using the **scan_cancel.php** function.

User permissions for the **scan_running_list.php** function are described below.

User Role	Permissions
Manager	View all running maps/scans. in subscription.
Unit Manager	View running maps/scans in user's business unit, including their own tasks and tasks run by other users in the same business unit.
Scanner	View running scans/maps in user's account.
Reader	No permission to view running maps/scans.

XML Report

The DTD for the XML running scans and maps list report returned by the **scan_running_list.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/scan_running_list.dtd
```

Appendix A provides information about the XML report generated by the **scan_running_list.php** function, including a recent DTD and XPath listing.

Cancel a Running Map

scan_cancel.php Function

The Scan Cancel API (**/msp/scan_cancel.php** is used to cancel a map in progress. It's not possible to cancel a map when it has the scan status "Loading". To cancel a map, use the following URL:

```
https://qualysapi.qualys.com/msp/scan_cancel.php?
  ref={referenceCode}
```

where the **ref={referenceCode}** parameter specifies the network map to be cancelled.

A map request for multiple domains issued using the **map-2.php** function, runs one map at a time, one domain at a time. If you cancel a running map for a domain using the **scan_cancel.php** function and there are multiple domains in the map target, the service cancels the maps for any remaining, undiscovered domains in the same map target. Note the map target may include multiple asset groups each of which may have multiple domains. See "Target Domains" for further information.

Note: This function can be used to cancel a running scan.

User permissions for the **scan_cancel.php** function are described below.

User Role	Permissions
Manager	Cancel any map in subscription.
Unit Manager	Cancel maps in user's business unit, including the user's own maps and maps run by other users in the business unit.
Scanner	Cancel maps in user's account.
Reader	No permission to cancel maps.

Parameters

The one parameter for **scan_cancel.php** is described below.

Parameter	Description
ref={value}	(Required) Specifies the map reference for the map to be cancelled (or a scan reference for the scan to be cancelled). A map reference starts with "map/". To find the appropriate reference, use the **scan_running_list.php** function.

Example

To cancel a map in progress with the code "map/987659876.19876", use the following URL:

```
https://qualysapi.qualys.com/msp/scan_cancel.php?
  ref=map/987659876.19876
```

XML Report

When you cancel a map, the **scan_cancel.php** returns an XML success message like this:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE GENERIC_RETURN SYSTEM
"https://qualysapi.qualys.com/generic_return.dtd">
<GENERIC_RETURN>
  <API name="scan_cancel" username="jim" at="2005-03-
22T22:32:20Z" />
  <RETURN status="SUCCESS">
  The map will be canceled ASAP.
  </RETURN>
</GENERIC_RETURN>
```

The DTD for the message returned by the **scan_cancel.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/generic_return.dtd
```

View Map Report List

map_report_list.php Function

The Map Report List API (**/msp/map_report_list.php**) is used to retrieve a list of map reports. To list saved map reports, use the following URL:

```
https://qualysapi.qualys.com/msp/map_report_list.php
```

You will receive a list of map reports in XML format. Each report has a reference code, a date, and the target domain. The network map report reference code can be used to retrieve a network map report using the **map_report.php** function.

User permissions for the **map_report_list.php** function are described below.

User Role	Permissions
Manager	View all saved map reports in the subscription.
Unit Manager	View saved map reports for domains in user's business unit.
Scanner	View saved map reports for domains in user's account.
Reader	View saved map reports for domains in user's account.

Parameters

The two optional parameters for **map_report_list.php** are described below.

Parameter	Description
last=yes	(Optional) Used to retrieve information only about the last saved map report. A valid value is "yes" to retrieve the last saved map report, or "no" (the default) to retrieve all map reports.
domain={target}	(Optional) Used to receive a list of all saved map reports for the specified target domain.

If you include both **domain={target}** and **last=yes**, you will receive information about the last saved map for the target domain.

Example

To receive information about the last saved network map for the domain "www.companyabc.com", specify a URL with the **last=yes** and the **domain={target}** parameters like this:

```
https://qualysapi.qualys.com/msp/map_report_list.php?
     domain=www.companyabc.com&last=yes
```

XML Report

The DTD for the XML map report list report returned by the **map_report_list.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/map_report_list.dtd
```

Appendix B provides information about the XML report generated by the **map_report_list.php** function, including a recent DTD and XPath listing.

Each entry in the map report list returned by the **map_report_list.php** function identifies a saved map report for a specific domain. If you issue a map request for multiple domains using the **map-2.php** function, there is a separate saved map report for each domain in the map target. For example, if you run the **map-2.php** function and your map target includes asset groups with a total of five domains, there are five separate map reports saved on the Qualys server. The separate maps may be retrieved using the **map_report.php** function, one at a time.

Retrieve a Saved Map Report

map_report.php Function

The Map Report API (**/msp/map_report.php**) is used to retrieve a saved map, when the map has the scan status "Finished". To retrieve a saved map report, use the following URL:

```
https://qualysapi.qualys.com/msp/map_report.php?
  ref={referenceCode}
```

The **ref={referenceCode}** parameter specifies the map report to be retrieved.

Each saved map report identifies map results for a specific domain. If you issue a map request for multiple domains using the **map-2.php** function, there is a separate saved map report for each domain in the map target. For example, if you run the **map-2.php** function and your map target includes a single domain and a single asset group with three domains, there are four separate saved map reports, one for each domain.

User permissions for the **map_report.php** function are described below.

User Role	Permissions
Manager	View saved map report in subscription.
Unit Managers	View saved map report for domain in user's business unit.
Scanner	View saved map report for domain in user's account.
Reader	View saved map report for domain in user's account.

Parameters

The one parameter for **map_report.php** is described below.

Parameter	Description
ref={value}	(Required) Specifies the map reference for the scan to be retrieved. A map reference starts with "map/". To find the appropriate reference, use the **map_report_list.php** function.

Example

To retrieve a saved map report with the reference code "map/987659876.19876", use the following URL:

```
https://qualysapi.qualys.com/msp/map_report.php?
  ref=map/987659876.19876
```

XML Report

The output from the **map_report.php** function is identical to the report produced by the **map.php** function. The DTD for the XML map report returned by these functions can be found at the following URL:

```
https://qualysapi.qualys.com/map.dtd
```

Typically a report returned from the **map_report.php** function will be returned quicker than a report returned from the **map.php** function because the network map request has already been processed.

Appendix B provides information about the XML report generated by the **map.php** and **map_report.php** functions, including a recent DTD and XPath listing.

Delete a Saved Map Report

scan_report_delete.php Function

The Scan Report Delete API (**/msp/scan_report_delete.php**) is used to delete a previously saved network map or scan report, when the scan status is "Finished". The reference code identifies the report to delete. To delete a saved map, use the following URL:

```
https://qualysapi.qualys.com/msp/scan_report_delete.php?
  ref={referenceCode}
```

where the **ref={referenceCode}** parameter specifies the map report to be deleted.

You can use the **scan_report_delete.php** function to delete a map report for a particular domain.

User permissions for the **scan_report_delete.php** function are described below.

User Role	Permissions
Manager	Delete saved map reports in the subscription.
Unit Manager	Delete saved map reports for domains in user's business unit, including the user's own maps and maps run by other users in the same business unit.
Scanner	Delete saved map reports in user's account.
Reader	No permission to delete map reports.

Parameters

The one parameter for **scan_report_delete.php** is described below.

Parameter	Description
ref={value}	(Required) Specifies the map reference for the map to be deleted. A map reference starts with "map/". To find the appropriate reference, use the **map_report_list.php** function.

Example

To delete a saved map report with the reference code "map/999666888.12345", use the following URL:

```
https://qualysapi.qualys.com/msp/scan_report_delete.php?
  ref=map/999666888.12345
```

XML Success Message

The **scan_report_delete.php** function returns an XML success message, like this:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE GENERIC_RETURN SYSTEM
"https://qualysapi.qualys.com/generic_return.dtd">
<GENERIC_RETURN>
   <API name="scan_report_delete.php" username="joe"
at="2002-04-18T11:14:38Z" />
<RETURN status="SUCCESS">
    The operation was successfully completed.
</RETURN>
</GENERIC_RETURN>
```

The DTD for the message returned by the **scan_report_delete.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/generic_return.dtd
```

CHAPTER 4

Account Preferences

Preference options in your Qualys account allow you to customize the behavior of the Qualys service. Using the Qualys API, you can view scheduled tasks (scans and maps), scan options in the default option profile, asset groups, and Scanner Appliances. Also, scheduled tasks and scan options can be edited.

This chapter describes how to use API functions to set preferences and view information about them. These topics are covered:

- Preferences Functions
- Scheduled Scans and Maps
- Scan Service Options
- View Scanner Appliance List
- View IP List
- View Domain List
- View Group List

When editing preferences for scheduled tasks and/or scan options, note that preference configurations affect the Qualys service — whether you are using the Qualys API or the Qualys user interface.

Preferences Functions

The preferences functions perform the following: schedule scans and/or maps to occur on a regular basis, set scan service options in the default option profile, view asset groups and Scanner Appliances in the user account.

Preferences are account-level configurations. The preferences functions display and edit configurations in the user account.

Scheduled Tasks — Maps and Scans

The **scheduled_scans.php** function is used to schedule tasks, both scans and maps, to occur on a regular basis. Scheduled tasks can be scheduled daily, weekly, and monthly. When a task is scheduled, the service starts the scan at the specified time.

The DTD for the XML document returned by the **scheduled_scans.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/scheduled_scans.dtd
```

Scan Options

The **scan_options.php** function is used to set scan options in the default option profile in the user account. These options allow you to specify ports to scan, and whether dead hosts and/or load balanced hosts will be scanned.

The DTD for the XML document returned by the **scan_options.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/scan_options.dtd
```

Scanner Appliance List

The iscanner_list.php function is used to view information about Scanner Appliances in the user account.

The DTD for the XML document returned by the **iscanner_list.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/iscanner_list.dtd
```

Asset Management

Qualys has released a new Asset Management Suite. This suite of API functions supports the management, assignment and tracking of assets for effective vulnerability management. It is recommended that you update to the new asset management functions which are described in Chapter 5, "Asset Management".

These asset management functions will be retired at a future date: **`ip_list.php`**, **`domain_list.php`** and **`group_list.php`**.

Function Name	Description
ip_list.php	View information about IP addresses that your account has access to. URL to report DTD: https://qualysapi.qualys.com/ip_list.dtd
domain_list.php	View information about domains that your account has access to. URL to report DTD: https://qualysapi.qualys.com/domain_list.dtd
group_list.php	View information about asset groups in the user account. An asset group may include domains for mapping, IPs for scanning security vulnerabilities, and Scanner Appliances for scanning internal networks. URL to report DTD: https://qualysapi.qualys.com/group_list.dtd

Scheduled Scans and Maps

scheduled_scans.php Function

Function Overview

The Scheduled Scans API (**/msp/scheduled_scans.php**) is used to add, list, and remove scheduled scan and map tasks on the Qualys server. Scheduled tasks can be defined to run daily, weekly, and monthly. The Qualys service automatically starts the scheduled tasks according to their specifications.

Express Lite: This API is available to Express Lite users.

The **scheduled_scans.php** function applies the default option profile in the user account to a scheduled task, unless another profile is specified for the task using the **option={name}** parameter.

Each scheduled task runs in local time defined for the task. You have the option to specify the local time as a time zone code or as a GMT shift value. When a time zone code that supports Daylight Saving Time (DST) is specified in the **time_zone_code** parameter with **observe_dst=yes**, the task observes DST by automatically adjusting the task's run time to reflect local time.

The Qualys service assigns a task ID to each scheduled task when the scheduled task is added. This task ID can be used to delete the scheduled task as described below in "Remove Task."

Each time a scheduled task successfully completes, the API user receives an email notification with scan or map results, unless this notification option is disabled in the user account. This email includes summary information plus a link to the detailed scan or map report. These results may also be returned using the **scan_report_list.php** and **scan_report.php** functions.

The reports produced by scheduled scans and maps are saved on the Qualys server. A scan report can be retrieved using the **scan_report.php** function. A map report can be retrieved using the **map_report.php** function. A report for a scheduled scan or map can be removed using the **scan_report_delete.php** function. The **scan_report_list.php** function lists reports for scheduled scans and maps.

Important: The **scheduled_scans.php** function does not check for validity of IP addresses and other task settings until run time — the first time the scheduled task is initiated. For example, in a case where you submit a request to add a new scheduled scan with an invalid IP address, the **scheduled_scans.php** function will create the new task without error or warning. Then, at run time the Qualys service will send an email notification stating "This scheduled task has been deactivated," with a reason for the deactivation. This email is sent to the registered Qualys user of the account.

Task Type Selection

The **type** parameter specifies the scheduled task type. When this parameter is not set, the default is **type=scan** for a scheduled scan.

Use the **type=map** parameter to add a scheduled map or request a list of scheduled maps. For example, to request a list of scheduled maps, use this URL:

```
https://qualysapi.qualys.com/msp/scheduled_scans.php?type=map
```

Use the **type=all** parameter to request a list of scheduled scans and maps together.

Task Target

The task target is defined using the **scan_target** and **asset_groups** parameters. For a scan task, you may specify a combination of IP addresses, IP address ranges, and asset groups. For a map task, you may specify a combination of domain names and asset groups.

The **scan_target** parameter is used to specify the target for a new scheduled scan or map. To add a scan task on IP addresses using the external scanner, use this URL:

```
https://qualysapi.qualys.com/msp/scheduled_scans.php?
add_task=yes&type=scan&scan_target={addresses}
```

To add a map task on two domains using a scanner appliance, use this URL:

```
https://qualysapi.qualys.com/msp/scheduled_scans.php?add_task=y
es&type=map&scan_target={domain1,domain2}&iscanner_name=name
```

Use the **asset_groups={title1,title2...}** parameter to specify asset groups for a task target.

For more information about the task target for a scheduled scan, see “Target Hosts” in Chapter 2. For a scheduled map, see “Target Domains” in Chapter 3.

Scanner Selection

Qualys supports internal and external scanning for both scan and map tasks. When a scanner is unspecified for a task, the Qualys External Scanners are used. A scanner option must be selected when the task target includes internal devices. You may select a Scanner Appliance name, the Default Scanner option for the default scanner in each target asset group. For a scheduled scan, you may select the All Scanners in Asset Group option for scanner parallelization.

The scanner parameters are described in the “Parameters” section. For more information, see “Scanner Selection for Scans” in Chapter 2 and “Scanner Selection for Maps” in Chapter 3.

User Permissions

User permissions for the **scheduled_scans.php** function are described below.

User Role	Permissions
Manager	Add tasks for all assets in the subscription. Remove all tasks. View all tasks in the subscription.
Unit Manager	Add tasks for assets in user's business unit. Remove tasks in user's business unit. View tasks in the subscription* (see below).
Scanner	Add tasks for assets in user's account. Remove user's scheduled tasks. View tasks in the subscription* (see below).
Readers	No permission to add and remove tasks. View tasks in the subscription* (see below).

* Qualys includes an account permission setting that restricts Unit Managers, Scanners, and Readers from viewing scheduled tasks on unassigned assets. For more details on this and user role-based permissions, see the Qualys online help.

Parameters

General Information

The parameters below apply to all scheduled tasks, both scans and maps. There are four **required** parameters to add a scheduled scan, and five **required** parameters for a scheduled map. The **iscanner_name** parameter is required when a Scanner Appliance is used.

Parameter	Description
add_task=yes	(Required to add a task) Used to add a scheduled task.
scan_title={title}	(Required to add a task) Specifies a title for the scheduled task.
type=scan | map | all	(Optional) Specifies the scheduled task type: **scan** for a scan task or **map** for a map task. If unspecified, the type is set to **type=scan**. For a scheduled map, this parameter must be set to **type=map**. The **all** type applies only when retrieving a list of scheduled tasks. For example, to receive a list of scheduled scans and maps, specify **type=all**.
active=yes | no	(Required to add a task) Specifies whether the scheduled task is active. When active, the scheduled task runs at the specified time. When inactive, the scheduled task does not run at its specified time.

Parameter	Description
scan_target={target}	(Optional) Specifies the task target. For a scheduled scan, specify IPs and/or IP ranges. For a scheduled map, specify one or more domain names. Multiple domain names must be comma separated. This parameter and/or **asset_groups** must be specified when adding a scheduled task. For a scheduled scan, see "Target Hosts" in Chapter 2 for further details. For a scheduled map, see "Target Domains" in Chapter 3.
asset_groups={title1,title2...}	(Optional) Specifies the titles of asset groups to be included in the scheduled task target. Multiple asset groups must be comma separated. This parameter and/or **scan_target** must be specified when adding a scheduled task. For a scheduled scan, see "Target Hosts" in Chapter 2 for further details. For a scheduled map, see "Target Domains" in Chapter 3.
exclude_ip_per_scan={value}	(Optional) Used to exclude certain IP addresses/ranges for the scheduled scan. One or more IPs/ranges may be specified. Multiple entries are comma separated. An IP range is specified with a hyphen (for example, 10.10.24.1-10.10.24.20).
iscanner_name={name}	(Optional) Specifies the name of the Scanner Appliance to be used for the scheduled task, when the task target has private use internal IPs. Using Express Lite, Internal Scanning must be enabled in your account. For a scheduled scan, see "Scanner Selection for Scans" in Chapter 2 for further details. For a scheduled map, see "Scanner Selection for Maps" in Chapter 3.
	One of these parameters may be specified in the same request: **iscanner_name**, **default_scanner**, or **scanners_in_ag** (for scheduled scan only).
runtime_http_header={value}	Set a custom value in order to drop defenses (such as logging, IPs, etc) when an authorized scan is being run. The value you enter will be used in the "Qualys-Scan:" header that will be set for many CGI and web application fingerprinting checks. Some discovery and web server fingerprinting checks will not use this header.

Parameter	Description
default_scanner=1	(Optional) Enables the default scanner feature, which is only valid when the task target consists of asset groups. A valid value is 1 to enable the default scanner, or 0 (the default) to disable it. Using Express Lite, Internal Scanning must be enabled in your account. For a scheduled scan, see "Scanner Selection for Scans" in Chapter 2 for further details. For a scheduled map, see "Scanner Selection for Maps" in Chapter 3.
	One of these parameters may be specified in the same request: **`iscanner_name`**, **`default_scanner`**, or **`scanners_in_ag`** (for scheduled scan only).
scanners_in_ag=1	(Optional) Enables the scanner parallelization feature for a scheduled scan, which is only valid when the scan target consists of asset groups. A valid value is 1 to enable scanner parallelization, or 0 (the default) to disable it. The scanner parallelization feature is not available for a scheduled map. Using Express Lite, Internal Scanning must be enabled in your account. See "Scanner Selection for Scans" in Chapter 2 for further details.
	One of these parameters may be specified in the same request: **`iscanner_name`**, **`default_scanner`**, or **`scanners_in_ag`** (for scheduled scan only).
option={title}	(Optional) Specifies the title of an option profile to be applied to the task, used when adding a task. The profile title must be defined in the user account, and it can have a maximum of 64 characters. If unspecified, the default option profile in the user account is applied. Note that custom option profiles can be defined only using the Qualys user interface. A selective vulnerability scan that includes a subset vulnerabilities (QIDs) in the KnowledgeBase may be specified. It's recommended that you include certain QIDs to ensure host information is available in your scan results and other reports. For more information, see "Scan Results and Host Scan Data" in Chapter 5.

Add Daily Task

The parameters listed below are **required** for daily tasks. See "Recurrence" for an optional parameter.

Parameter	Description
occurrence=daily	(Required) Specifies that the task will occur daily.
frequency_days={value}	(Required) Specifies that the task will run every N days, where N is a number of days. A valid value is an integer from 1 to 365.
{start time parameters}	(Required) Specifies when the task will start. See "Start Time" for a complete list of parameters.

Add Weekly Task

The parameters listed below are **required** for a weekly task. See "Recurrence" for an optional parameter.

Parameter	Description
occurrence=weekly	(Required) Specifies that the task will occur weekly.
frequency_weeks={value}	(Required) Specifies that the task will run every N weeks, where N is a number of weeks. A valid value is an integer from 1 to 52.
weekdays={value}	(Required) Specifies on which weekdays the task will run. One or more days may be specified. A valid value is: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday. Multiple days are comma separated.
{start time parameters}	(Required) Specifies when the task will start. See "Start Time" for a complete list of parameters.

Add Monthly Task — Nth Day of Month

The parameters listed below are **`required`** for a monthly task to be run on the Nth day of the month where N is a day of the month that you specify. For example, you can setup a monthly task to run on the 15th day of each month. See "Recurrence" for an optional parameter.

Parameter	Description
occurrence=monthly	(Required) Specifies that the scheduled task will occur monthly.
frequency_months={value}	(Required) Specifies that the task will run, as in every N months, where N is a number of months. A valid value is an integer from 1 to 12.
day_of_month={value}	(Required) Specifies the day of the month to run. A valid value is an integer from 1 to 31.
{start time parameters}	(Required) Specifies when the task will start. See "Start Time" for a complete list of parameters.

Add Monthly Task — Weekday in Nth Week of Month

The parameters listed below are **`required`** for a monthly task to be run on a day of the week (for example Monday, Tuesday) in a particular week of the month. For example, you can setup a monthly task to run on the second Tuesday of the month. See "Recurrence" for an optional parameter.

Parameter	Description
occurrence=monthly	(Required) Specifies that the scheduled task will occur monthly.
frequency_months={value}	(Required) Specifies that the task will run every N months, where N is a number of months. A valid value is an integer from 1 to 12.
day_of_week={value}	(Required) Specifies the day of the week when the task will run. A valid value is an integer from 0 to 6, where 0 is Sunday and 6 is Saturday.
week_of_month={value}	(Required) Specifies the Nth week of the month, when the task will run. A valid value is: first, second, third, fourth, or last.
{start time parameters}	(Required) Specifies when the task will start. See "Start Time" for a complete list of parameters.

Start Time

The parameters listed below specify start time settings used to launch the scheduled task. Some start time parameters are **required** for all scheduled tasks as indicated.

Parameter	Description
time_zone_code={value}	(Optional) Specifies the time zone for the task as a pre-defined code. For example, the time zone code for US California is US-CA. Time zone codes must be specified in upper case. Valid time zone codes are provided in the "Time Zone Code List" returned by the **time_zone_code_list.php** function. For a time zone code that supports Daylight Saving Time, you can specify **observe_dst=yes** so that the task is updated automatically to reflect local time. This parameter or **time_zone** must be specified. See "Time Zone Selection" below for further details.
observe_dst={yes}	(Optional) Enables the observe Daylight Saving Time (DST) feature for the task. This feature can be enabled when the time zone code specified in **time_zone_code** supports DST. When enabled, the service automatically adjusts the start time for the task to reflect local time. To enable this feature, specify **observe_dst=yes**. Some locales do not support DST, like Arizona and Hawaii. For these locales, if you specify a time zone code with observe_dst=yes, the function returns an error. This parameter may be specified with **time_zone_code**. (This parameter is invalid when specified with **time_zone**.)
time_zone={value}	(Optional) Specifies the time zone for the task as a GMT shift value. This is the difference, in hours, between GMT and the local time zone. A valid value is an integer from -12 to 12. For example, the GMT shift for Pacific Standard Time (PST) in California is -8. This parameter cannot be used when the timezone has a 30 or 15 minute offset (for example GMT-930 or GMT+1245). This parameter or **time_zone_code** must be specified. See "Time Zone Selection" below for further details. Note: This parameter is available for backward compatibility and may not be supported in future releases.
start_date={mm/dd/yyyy}	(Optional) Specifies the start date in mm/dd/yyyy format. By default, the start date is the date when the task is created.

Parameter	Description
start_hour={hour}	(Required) Specifies the hour when the task will start. The hour variable is an integer from 0 to 23, where 0 represents 12 AM, 7 represents 7 AM, and 22 represents 10 PM.
start_minute={minute}	(Optional) Specifies the minute when the task will start. A valid value is an integer from 0 to 59.
end_after={value}	(Optional) Specifies the number of hours to wait for a map or scan to complete before deactivating the task. By default the service does not deactivate tasks until they complete. A valid value is an integer from 1 to 48.

Recurrence

The recurrence parameter listed below is optional. By default the task does not end unless it is deactivated or deleted.

Parameter	Description
recurrence={value}	(Optional) Specifies the number of times the task will be run before it is deactivated. A valid value is an integer from 1 to 99. For example, if you set **`recurrence=2`**, the scheduled task will be deactivated after it runs 2 times.

Remove Task

The following parameters are **`required`** to remove a scheduled task. Both parameters must be specified. When these parameters are set, the function removes the specified scheduled task and returns an XML success message.

Parameter	Description
drop_task=yes	(Required) Used to delete a scheduled task. A valid value is "yes" to delete the task or "no" (the default) to not delete the task.
task_id={taskID}	(Required) Specifies the task ID of the task to be deleted. The Qualys service assigns a task ID to each scheduled task when the task is added.

If you remove a scheduled task, any saved reports for the scheduled task remain on the Qualys server.

Time Zone Selection

When adding a task, you must identify local time by specifying either a time zone code or a GMT shift value using the parameters described below. These are mutually exclusive parameters which cannot be used together.

Time Zone Parameters

For the **time_zone_code** parameter, you specify a time zone code that corresponds to local time. Refer to the "Time Zone Code List" below to select an appropriate code. For example if the task will run in New York, then you specify the code "US-NY". Many time zones, like New York, observe DST. If you specify a code for a time zone that supports DST, you have the option to enable the observe Daylight Saving Time (DST) feature so the task is updated automatically to reflect local time. To enable this feature. specify **observe_dst=yes**.

For the **time_zone** parameter, you specify a GMT shift, like -8 for Pacific Standard Time in California, that corresponds to local time. When the timezone has a 30 or 15 minute offset, then the **time_zone** parameter cannot be used. When specified, the service automatically determines the appropriate time zone code for the task and includes this in scheduled scans reports. See "Automatic Translation — GMT Shift to Time Zone Code" in Appendix C for further information. Note this parameter has been available in previous releases and is supported for backward compatibility.

Time Zone Code List

The **time_zone_code_list.php** function provides a list of all available time zone codes that can be specified with the **time_zone_code** parameter.

To retrieve a list of time zone codes, use this URL:

```
https://qualysapi.qualys.com/msp/time_zone_code_list.php
```

The DTD for the XML document returned from **time_zone_code_list.php** can be found at the following URL:

```
https://qualysapi.qualys.com/time_zone_code_list.dtd
```

Sample time zone code list output is shown below:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCHEDULEDSCANS SYSTEM
"https://qualysapi.qualys.com/time_zone_code_list.dtd">
<TIME_ZONES>
  <TIME_ZONE>
    <TIME_ZONE_CODE>AS</TIME_ZONE_CODE>
    <TIME_ZONE_DETALS><![CDATA[(GMT-1100) American Samoa: Pago
Pago]]></TIME_ZONE_DETALS>
    <DST_SUPPORTED>0</DST_SUPPORTED>
</TIME_ZONE>
<TIME_ZONE>
    <TIME_ZONE_CODE>UM2</TIME_ZONE_CODE>
    <TIME_ZONE_DETALS><![CDATA[(GMT-1100) Midway Islands
(U.S.)]]></TIME_ZONE_DETALS>
    <DST_SUPPORTED>0</DST_SUPPORTED>
</TIME_ZONE>

<TIME_ZONE>
    <TIME_ZONE_CODE>NU</TIME_ZONE_CODE>
    <TIME_ZONE_DETALS><![CDATA[(GMT-1100) Niue: Alofi]]>
</TIME_ZONE_DETALS>
    <DST_SUPPORTED>0</DST_SUPPORTED>
</TIME_ZONE>
<TIME_ZONES>
```

Each <TIME_ZONE> element identifies a time zone properties, including the code, in the sub-elements described below.

Element	Description
<TIME_ZONE_CODE>	A time zone code. These are pre-defined codes.
<TIME_ZONE_DETAILS>	Text describing the time zone.
<DST_SUPPORTED>	A value (0 or 1) indicating whether the time zone supports Daylight Saving Time (DST). 1 is reported when DST is supported, and 0 is reported when DST is not supported.

Examples

Scheduled Tasks Lists

To receive an XML document including a list of all scheduled scans, use this URL:

```
https://qualysapi.qualys.com/msp/scheduled_scans.php
```

To receive an XML document with a list of all scheduled scans and maps, use this URL:

```
https://qualysapi.qualys.com/msp/scheduled_scans.php?type=all
```

To receive an XML document including a list of all scheduled maps, use this URL:

```
https://qualysapi.qualys.com/msp/scheduled_scans.php?type=map
```

Scheduled Scans

The URL below adds a daily scan called "Scan1" that is defined to scan IP address "10.20.30.3". "Scan1" is scheduled to start at 2 PM every day in Los Angeles, California where DST is observed. The URL below includes all parameters required to add "Scan1" as an active scan:

```
https://qualysapi.qualys.com/msp/scheduled_scans.php?add_task=y
es&scan_title=Scan1&active=yes&scan_target=10.20.30.3&iscanner_
name=scanner1&occurrence=daily&frequency_days=1&time_zone_code=
US-CA&observe_dst=yes&start_hour=14&start_minute=0
```

To add a daily scan called "My Daily Scan" that is defined to scan IP address "10.10.10.3", specify the URL below. This daily scan is scheduled to start at 4 PM every day in the California time zone. The URL below includes all required parameters:

```
https://qualysapi.qualys.com/msp/scheduled_scans.php?add_task=y
es&scan_title=My+Daily+Scan&active=yes&scan_target=10.10.10.3&i
scanner_name=scanner1&occurrence=daily&frequency_days=1&time_zo
ne_code=US-CA&observe_dst=yes&start_hour=14&start_minute=0
```

The URL below adds a weekly scan called "Scan2" that is defined to scan the asset groups "Finance" and "Operations". "Scan2" is scheduled to start at 10 AM every 2nd Tuesday in Paris, France where DST is observed. The URL below includes all required parameters:

```
https://qualysapi.qualys.com/msp/scheduled_scans.php?add_task=y
es&scan_title=Scan2&active=yes&asset_groups=Finance,Operations&
iscanner_name=scanner2&option=RV10+Options&occurrence=weekly&fr
equency_weeks=2&weekdays=Tuesday&time_zone_code=FR&observe_dst=
yes&start_hour=10&start_minute=0&recurrence=90
```

The URL below adds a monthly scan called "Scan3" that is defined to scan 3 asset groups with the default scanner enabled. "Scan3" starts every 2 months on the 2nd Friday of the month at 6 PM in New York City where DST is observed.

```
https://qualysapi.qualys.com/msp/scheduled_scans.php?add_task=y
es&scan_title=Scan3&active=yes&asset_groups=Critical+Group+4,Cr
itical+Group+5,Critical+Group+6&default_scanner=1&occurrence=mo
nthly&frequency_months=2&day_of_week=5&week_of_month=2&time_zon
e_code=US-NY&observe_dst=yes&start_hour=18&start_minute=0
```

The URL below adds a monthly scan called "My Scheduled Scan" that uses the scanner parallelization feature.

```
https://qualysapi.qualys.com/msp/scheduled_scans.php?
add_task=yes&scan_title=My+Scheduled+Scan&active=yes&
asset_groups=Group+A,Group+B,Group+C&scanners_in_ag=1&
occurrence=monthly&frequency_months=2&day_of_week=5&
week_of_month=2& time_zone_code=US-NY&
observe_dst=yes&start_hour=18& start_minute=0
```

The URL below removes a scheduled scan with the task ID "6703". Two parameters are required as shown.

```
https://qualysapi.qualys.com/msp/scheduled_scans.php?drop_task=
yes&task_id=6703
```

Scheduled Maps

To add a weekly map called "My Weekly Map" to perform discovery on "mydomain.com", specify the URL below. This weekly map runs every 8 weeks and starts on Sunday at 2 AM in Tokyo, Japan.

```
https://qualysapi.qualys.com/msp/scheduled_scans.php?add_task=y
es&scan_title=My+Weekly+Map&active=yes&type=map&scan_target=myd
omain.com&iscanner_name=scanner5&occurrence=weekly&frequency_we
eks=8&weekdays=Sunday&time_zone_code=JP&start_hour=2&start_minu
te=0
```

The URL below removes a scheduled map with the task ID "11155". Note that two parameters are required as shown.

```
https://qualysapi.qualys.com/msp/scheduled_scans.php?
drop_task=yes&task_id=11155
```

XML Report

The DTD for the XML results returned by the **scheduled_scans.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/scheduled_scans.dtd
```

This XML document supports reporting on scheduled scans and maps.

Appendix C provides information about the XML report generated by the **scheduled_scans.php** function, including a recent DTD and XPath listing.

Scan Service Options

scan_options.php Function

The **scan_options.php** function is used to view and edit scan options in the default options profile in the user account. This function allows you to specify TCP ports to scan, and whether dead hosts and/or load balanced hosts will be scanned.

To send a scan service option request to the Qualys server, use this URL:

```
https://qualysapi.qualys.com/msp/scan_options.php?{parameters}
```

where **{parameters}** represents one or more parameters in the form of name-value pairs.

To list the parameters for the scan service options, specify this URL:

```
https://qualysapi.qualys.com/msp/scan_options.php
```

Upon completion of the function, an XML scan options report is returned.

The scan service settings are stored persistently on the Qualys server in the default options profile (in the user account). You can update one or all of the settings at any time using the **scan_options.php** function. If a name-value pair is missing, the previous setting is used. If one field is invalid or would otherwise produce an error, all subsequent change attempts will not occur.

User permissions for the **scan_options.php** function are described below.

User Role	Permissions
Manager	Set scan options in the default options profile. View settings in default option profile.
Unit Manager	No permission to set scan options. View settings in default options profile.
Scanner	No permission to set scan options. View settings in default options profile.
Reader	No permission to set scan options. View settings in default options profile.

Note: The Performance Level settings provide users with greater control over the overall performance level for both scans and maps. The Bandwidth Impact (set using the **bandwidth** parameter) was a scan option in Qualys API Versions 3.4 and earlier, is no longer supported.

Parameters

Three parameters can be specified with the **scan_options.php** function.

Parameter	Description
scandeadhosts={yes | **no**}	Supports scanning dead hosts. By default, dead hosts are not scanned.
loadbalancer={yes | **no**}	Checks for load balanced hosts during scans. When a load balancer is detected, all systems behind it are also scanned for vulnerabilities. By default, load balanced hosts are not checked.
ports={**default** | full | {range}}	Specifies TCP ports to scan. By default, the service scans the most commonly-used TCP ports.

Scan Dead Hosts

The **scandeadhosts=yes** parameter is used to scan dead hosts. For a new account, the service does not scan dead hosts.

The syntax for this parameter is below:

```
scandeadhosts=yes|no
```

During a scan, the scan service determines whether a host is dead or alive. The service checks network services on the host, such as ping, SMTP, SSH, and HTTP, and tries to connect using each one. If none of the network services respond, the scan service determines that the host is "dead" and no further security analysis occurs for that host.

If you set **scandeadhosts=yes**, the scan service will perform all the usual tests on dead hosts in addition to live ones.

Load Balancer Check

The **loadbalancer** parameter is used to check for load balanced hosts. For a new account, the service does not check for load balanced hosts.

The syntax for this parameter is below:

```
loadbalancer=yes|no
```

If you set **loadbalancer=yes**, the scan service checks for load balanced hosts. When a load balancer is detected, all systems behind it are also scanned for vulnerabilities.

Scan TCP Ports

The **ports** parameter is used to specify which TCP ports are scanned.

The syntax for this parameter is below:

```
ports=default|full|{range}
```

The valid name-value pairs for the ports parameter are below.

Parameter name-value pairs	Description
ports=default	Scan using the Standard TCP Ports list, including the most commonly-used ports (about 1,900 ports). This ports list is available in the Qualys user interface.
ports=full	Full scan of all TCP ports. Note: This setting may increase scan time and is not recommended for Class C or larger networks.
ports={range}	Scan a custom list of TCP ports, including individual ports and/or port ranges. Use the dash (-) character to separate the start and end ports in the range. Use the comma (,) to separate port numbers and ranges.

Examples

To scan dead hosts, use this URL:

```
https://qualysapi.qualys.com/msp/scan_options.php?scandeadhosts=yes
```

To check for load balancer hosts and scan all systems behind them, use this URL:

```
https://qualysapi.qualys.com/msp/scan_options.php?loadbalancer=yes
```

To scan the Standard TCP port list, use this URL:

```
https://qualysapi.qualys.com/msp/scan_options.php?ports=default
```

To scan only TCP ports 80 and 443, use this URL:

```
https://qualysapi.qualys.com/msp/scan_options.php?ports=80,443
```

XML Report

The DTD for the XML scan options report returned by the **scan_options.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/scan_options.dtd
```

Appendix C provides information about the XML report generated by the **scan_options.php** function, including a recent DTD and XPath listing.

View Scanner Appliance List

iscanner_list.php Function

The Scanner Appliances List API (**/msp/iscanner_list.php**) is used to view information about the Scanner Appliances in the user account.

Express Lite: This API is available to Express Lite users when Internal Scanning is enabled in your account.

For each Scanner Appliance this information is provided: scanner appliance ID and friendly name, IP address and status. The status is reported as "online" if the Scanner Appliance responded to the most recent heartbeat check and contacted the Qualys Security Operations Center at that time; the status is "offline" if the appliance did not respond to the most recent heartbeat check and did not contact the Qualys Security Operations Center at that time. The service automatically performs a heartbeat check every 4 hours.

A Scanner Appliance available in your account after it has been installed following the three-step Quick Start that is described in the *Qualys Scanner Appliance User Guide*. For a user other than a Manager, a Manager must add the Scanner Appliance to your account after installation.

To view Scanner Appliances in the user account, use the following URL:

```
https://qualysapi.qualys.com/msp/iscanner_list.php
```

User permissions for the **iscanner_list.php** function are described below.

User Role	Permissions
Manager	View all scanner appliances in the subscription.
Unit Manager	View scanner appliances in user's business unit.
Scanner	View scanner appliances in user's account.
Reader	View scanner appliances in user's account.

XML Report

The DTD for the XML Scanner Appliance list report returned by the **iscanner_list.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/iscanner_list.dtd
```

Appendix C provides information about the XML report generated by the **iscanner_list.php** function, including a recent DTD and XPath listing.

View IP List

ip_list.php Function

The **ip_list.php** function is used to view a list of IP addresses in the user account. To view the IP list, use the following URL:

```
https://qualysapi.qualys.com/msp/ip_list.php
```

When no parameters are specified with an **ip_list.php** request, the function returns a list of IP ranges. Each range is defined by a start IP address and an end IP address.

There are two optional parameters, which may be used to retrieve host details: **detailed_results** and **detailed_no_results**. For information on these parameters, see "View Asset IP List" in Chapter 5, "Asset Management".

User permissions for the **ip_list.php** function are the same as the user permissions for the new **asset_ip_list.php** function. See below for information on this new function.

The DTD for the XML IP list report returned by the **ip_list.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/ip_list.dtd
```

Appendix D provides information about the XML report generated by the **ip_list.php** function and the new **asset_ip_list.php** function.

New asset_ip_list.php Function

Qualys has released a new function called **asset_ip_list.php**. It is recommended that you update to the new function which is described in Chapter 5, "Asset Management".

The **ip_list.php function** will be retired at a future date.

View Domain List

domain_list.php Function

The **domain_list.php** function is used to view a list of domains in the user account. To view the domain list, use the following URL:

```
https://qualysapi.qualys.com/msp/domain_list.php
```

User permissions for the **domain_list.php** function are the same as the user permissions for the new **asset_domain_list.php** function. See below for information on this new function.

The DTD for the XML domain list report returned by the **domain_list.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/domain_list.dtd
```

Appendix D provides information about the XML report generated by the **domain_list.php** function and the new **asset_domain_list.php** function.

New asset_domain_list.php Function

Qualys has released a new function called **asset_domain_list.php**. It is recommended that you update to the new function which is described in Chapter 5, "Asset Management".

The **domain_list.php function** will be retired at a future date.

View Group List

group_list.php Function

The Asset Group List API (**/msp/group_list.php)** is used to view the asset groups in the user account. To view the group list, use the following URL:

```
https://qualysapi.qualys.com/msp/group_list.php
```

Express Lite: This API is available to Express Lite users.

User permissions for the **group_list.php** function are the same as the user permissions for the new **asset_group_list.php** function. See below for information on the new function.

The DTD for the XML group list report returned by the **group_list.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/group_list.dtd
```

Appendix C provides information about the XML report generated by the **group_list.php** function.

New asset_group_list.php Function

Qualys has released a new function called **asset_group_list.php**. This new function lists additional asset group data, including business information, CVSS Environmental Metrics, and assigned users.

It is recommended that you update to the new function which is described in Chapter 5, "Asset Management".

The **group_list.php function** will be retired at a future date.

CHAPTER 5

Asset Management

The Qualys API provides many ways to manage assets in the user account. Several functions allow you to manage assets in the subscription (IP addresses and domains), manage asset groups, search assets based on attributes, and download asset reports.

The asset management capabilities that available using the Qualys API are described in this chapter. A quick reference to these function is below.

Options	Capabilities	Functions
Manage Assets in Subscription	Add/Edit Asset IPs View Asset IP List Add/Edit Domains View Asset Domain List	asset_ip.php asset_ip_list.php asset_domain.php asset_domain_list.php
Manage Asset Groups	Add/Edit Asset Group View Asset Group List Delete Asset Group	asset_group.php asset_group_list.php asset_group_delete.php
Search Assets	Search Assets by Attributes	asset_search.php
Download Asset Reports	Download Asset Data Report Report Template List ---------- Download Asset Range Info Report	asset_data_report.php report_template_list.php ---------- asset_range_info.php

Asset management configurations are available in both the Qualys user interface and the Qualys API. For example if you add an IP range to the subscription, the IP range is listed in the user interface as well as the asset IP list returned by the **`asset_ip_list.php`** function. These IP addresses are available to all users based on their user role and associated asset permissions.

Asset Management Functions

A summary of the asset management functions that are available in the Qualys API are described below.

Manage Assets in Subscription

Function Name	Description
asset_ip.php	Add/edit asset IP addresses and related data, such as host tracking method, owner, user-defined attributes and comments. XML results returned using the generic return DTD: https://qualysapi.qualys.com/generic_return.dtd
asset_ip_list.php	View a list of asset IP addresses which the API user has permission to access. (Note: This function was formerly named ip_list.php.) XML results returned using the IP list DTD: https://qualysapi.qualys.com/ip_list.dtd
asset_domain.php	Add/edit asset domains and related netblocks. XML results returned using the generic return DTD: https://qualysapi.qualys.com/generic_return.dtd
asset_domain_list.php	View a list of asset domains which the API user has permission to access. (Note: This function was formerly named domain_list.php.) XML results returned using the domain list DTD: https://qualysapi.qualys.com/domain_list.dtd

Manage Asset Groups

Function Name	Description
asset_group.php	Add/edit an asset group and its related data, including assigned IP addresses, domains, business information and scanner appliances. XML results returned using the generic return DTD: https://qualysapi.qualys.com/generic_return.dtd
asset_group_list.php	View a list of asset groups. (Note: This function was formerly named domain_list.php.) XML results returned using the asset group list DTD: https://qualysapi.qualys.com/asset_group_list.dtd
asset_group_delete.php	Delete an asset group. XML results returned using the generic return DTD: https://qualysapi.qualys.com/generic_return.dtd

Search Assets

The asset search function (asset_search.php) is used to search for assets that the user account has permission to access, and return search results. The search results are returned using the asset search DTD (asset_search_report.dtd).

Download Asset Reports

Function Name	Description
asset_data_report.php	Download an asset data report for an automatic report template which is available in the API user's account. To obtain a list of report templates in the user account, use report_template_list.php. XML results returned using the asset data report DTD: https://qualysapi.qualys.com/asset_data_report.dtd
asset_range_info.php	Download an asset data report for a range of assets specified with the request. The report target may include a combination of IP addresses, ranges, and asset groups. XML results returned using the asset group list DTD: https://qualysapi.qualys.com/asset_range_info.dtd

Automatic Host Scan Data

Scan data is part of a host's vulnerability history, which is saved separately from saved scan results. The Qualys API references host scan data to search assets (asset_search.php), list IP addresses with detailed results (asset_ip_list.php), and to download reports such as the asset data report (asset_data_report.php), the asset range info report (asset_range_info.php), the host information report (get_host_info.php) and the tickets report (get_tickets.php).

Scan Results and Host Scan Data

It is important to note that host scan data is based on saved scan results. When scan results become available from a scan request (on demand or scheduled), Qualys saves the scan data in two forms: saved scan results and host scan data. Saved scan results provide a task based profile with scan data as of the time when the scan task was run. Host scan data is optimized for retrieval and report generation to provide a current profile with scan data as of the time when the scan data was retrieved.

Scan results may be deleted so that they are no longer available for viewing in the user account. Using the Qualys API, scan results may be deleted using the scan report delete function (scan_report_delete.php). Using the Qualys user interface, scan results may be deleted manually or automatically based on user configurations. Note however that deleting scan results does not delete any host scan data. This means that you can delete all scan results for a particular host and still access the host scan data for that host in asset reports that are generated using automatic data selection. To remove host scan data, the host must be purged using the Qualys user interface. See the Qualys online help for information on how to purge hosts.

No Host Scan Data

Hosts that have not been scanned do not have associated scan data. A host that is in your account may not have scan data even though it was scanned at some time. A host may not have scan data because the host was included in a scan target however the host was identified as not alive during host discovery and thus not scanned. A host will not have scan data if it was scanned, then purged, and not scanned again.

When no host scan data is available for target hosts, Qualys does not include these hosts in the XML results, such as asset search results or asset scan reports (automatic), produced using the Qualys API and/or the Qualys user interface.

Selective Vulnerability Scans and Partial Host Scan Data

A selective vulnerability scan performs vulnerability assessment only for the specific vulnerability checks configured in the profile that is applied to the scan task — on demand or scheduled. When setting up a profile for a selective vulnerability scan, you may wish to include certain vulnerability checks to ensure that target host information, including operating system and services running, are available in your scan results.

It's recommended best practice to include these vulnerability checks to obtain basic host information available in your account.

Host Scan Data	Vulnerability Check Title (QID)
Operating System	"Operating System Detected" (QID 45017)
TCP services	"Open TCP Services List" (QID 82023)
UDP services	"Open UDP Services List" (QID 82004)
DNS host name	"DNS Host Name" (QID 6)
NetBIOS host name	"NetBIOS Host Name" (QID 82044)

For host management, it may be desirable to find additional host settings, which are returned by specific vulnerability checks. Using the Qualys user interface, you can search for vulnerabilities to include.

Host Tracking Method

When a host is tracked by DNS or NetBIOS, the appropriate host name is gathered during the scanning process, reported in scan results, and saved with the host scan data. If a host name is not gathered, the host is not scanned and scan results are not returned.

Each host in the subscription is assigned a tracking method: IP address, DNS host name or NetBIOS host name. The tracking method is included in scan results and host scan data. Initially, when a subscription is created with IP addresses, the hosts are assigned the IP address tracking method. Using the asset IP address function (asset_ip.php), API users can specify the tracking method when adding and editing IP addresses. Managers can add IP addresses (up to the subscription limit) for a specified tracking method. All Managers and Unit Managers, who have asset permission, can edit hosts to change the assigned tracking method.

After a host is scanned, a user may attempt to change the tracking method to DNS or NetBIOS. This request prompts Qualys to reference the host scan data entry in the user account. In order to commit the change, the service must find an associated host name in the host scan data entry, and must resolve the target IP address to one host name. For more information, see "Add/Edit Asset IPs" later in this chapter.

To scan hosts tracked by DNS and/or NetBIOS it's required that the scanning engine reference the appropriate host names for all target hosts from the host scan data in the user account. When scanning hosts tracked by DNS, be sure that your DNS servers are configured to communicate with Qualys scanners. DNS servers must be able to resolve the scan target IP addresses to DNS host names. When scanning hosts by NetBIOS, be sure to include UDP port 137 in scan options (options profile). UDP port 137 is included in the "Initial Options" option profile provided by the service. If you use a custom profile, this port is included when the "Scanned UDP Ports" scan option is set to Standard Scan, Light Scan or Full.

Add/Edit Asset IPs

asset_ip.php Function

Function Overview

The Asset IP API (**`/msp/asset_ip.php`**) is used to manage (add and edit) asset IP addresses and related data in the subscription. Related data for each host includes the tracking method, owner, user-defined attributes such as Location, Function and Asset Tag, and comments. The IP addresses in the subscription may be used as targets for vulnerability scanning and reporting. Using the Qualys user interface, Managers and Unit Managers can assign these IP addresses to other users.

Express Lite: This API is available to Express Lite users.

This API enables a Manager to make requests to add or edit IP addresses in the subscription. A Unit Manager with the add asset permission may add IP addresses to their business unit. Any Unit Manager can edit IP addresses in their business unit, regardless of whether the Unit Manager has the add assets permission. When you make a request, the function performs the requested update and returns an XML document indicating the status of the request.

Host Tracking

Every host IP address in the subscription is assigned a tracking method: IP address, DNS host name or NetBIOS host name. In a new subscription, all hosts are tracked by IP address. The assigned tracking method determines how the host will be reported in scan reports. Hosts assigned a tracking method of DNS or NetBIOS host name will be listed in alphabetical order by host name. Hosts assigned a tracking method of IP address will be listed in numerical order by IP address.

Using **`asset_ip.php`**, you can assign another tracking method to one or more host IP addresses using the **`tracking_method`** parameter. For each request, one tracking method may be assigned to the target IP addresses specified in the request. For an add request, the new IP addresses are tracked by IP address by default unless the **`tracking_method`** parameter is used to specify another method.

Qualys creates host scan data entries (records) for each scan task. Host scan data is a part of a host's vulnerability history, which is saved separately from saved scan results. Each host scan data entry identifies the host information including it's IP address, DNS host name and NetBIOS host name if available.

Note these important issues when changing the tracking method. You can change the tracking method to "dns" or "netbios" when the service can: 1) Find an associated host name (DNS or NetBIOS) in the scan data entry for each target host, and 2) Resolve each target IP address to one host name (DNS or NetBIOS) based in a host scan data entry.

The tracking method can be changed to DNS or NetBIOS when the associated host name was gathered in a previous scan. It's possible that the host IP address was scanned, however the DNS or NetBIOS host name was not gathered and thus not part of the host scan data entry.

Numerous scan tasks on the same IP address may gather different DNS and NetBIOS host names. In this case, your account will have multiple host scan data entries. To change the tracking method, there can be only one scan data entry for each host. If there are multiple entries for the same IP address, you must purge scan data entries using the Qualys user interface before sending an edit request using **`asset_ip.php`** to change the tracking method for the host.

User Permissions

User permissions for the **`asset_ip.php`** function are described below.

User Role	Permissions
Manager	Add/Edit IP addresses and related data in the subscription.
Unit Manager	Add IP addresses and related data in the subscription when the Unit Manager has the add assets permission. Edit IP addresses and related data in the subscription when IP addresses are in asset groups assigned to the Unit Manager's business unit. Any Unit Manager can edit IP addresses in their own business unit, regardless of whether the Unit Manager has the add assets permission.
Scanner	No permission to add/edit asset IP addresses and related data.
Reader	No permission to add/edit asset IP addresses and related data.

Parameters

The parameters for **asset_ip.php** are described below.

Parameter	Description
action=add|edit	(Required) A flag indicating an add or edit request. Specify "add" to add a new IP address, or "edit" to edit an existing IP address.
host_ips={addresses}	(Required) Specifies one or more IP addresses to add or edit. You may enter a combination of individual IPs and IP ranges. CIDR notation is supported. Multiple entries are comma separated. For each API request, you can specify an unlimited number of IPs, if your subscription permits. For example, an entire class A network can be added using "10.10.10.0/8". Note: The maximum number of IP addresses that can be added depends on the number of IPs purchased for the subscription. Please contact your Qualys account representative or Qualys Support if you wish to add more IP addresses to your subscription. You may enter only one IP address when this parameter is specified with **host_dns** or **host_netbios**.
ag_title={title}	(Required for add request by Unit Managers only) Specifies the title of an asset group which is assigned to your business unit. When specified, the IP addresses will be added to: 1) the subscription, and 2) the asset group, making them available to Unit Managers in your business unit and other users assigned the asset group. This parameter is invalid for add requests by Managers, and all edit requests.
host_dns={hostname}	(Optional for edit request only) Specifies a DNS host name to identify a specific host scan data entry (record) that you wish to edit. This parameter is used when there are multiple host scan data entries with the same IP address. This parameter may be specified only for an edit request (and is invalid for an add request). This parameter cannot be specified with **tracking_method**.

Parameter	Description
host_netbios={hostname}	(Optional for edit request only) Specifies a NetBIOS host name to identify a specific host scan data entry (record) that you wish to edit. This parameter is used when there are multiple host scan data entries with the same IP address. This parameter may be specified only for an edit request (and is invalid for an add request). This parameter cannot be specified with **`tracking_method`**.
tracking_method={method}	(Optional) Specifies the host tracking method assigned to the IP addresses specified in the **`host_ips`** parameter. For an add request, the default method is IP. A valid tracking method is: "ip" (for IP address), "dns" (for DNS host name) or "netbios" (for NetBIOS host name). Initially in a new subscription, IP addresses are assigned the IP tracking method. This parameter is invalid if specified with **`host_dns`** or **`host_netbios`**. Note these important issues when changing the tracking method. You can change the tracking method to "dns" or "netbios" when the service can: 1) Find an associated host name (DNS or NetBIOS) in the scan data entry for each target host, and 2) Resolve each target IP address to one host name (DNS or NetBIOS) in a host scan data entry.
owner={owner}	(Optional) Specify the login name of the asset owner. For an add request, a Manager account must be specified. For an edit request, any user account that has permission to the host IP addresses may be specified.
ud1={attribute1}	(Optional) Specify a value for user-defined host attribute 1. Initially the name of this attribute is "Location" and it may be customized using the Qualys user interface.
ud2={attribute2}	(Optional) Specify a value for the user-defined host attribute 2. Initially the name of this attribute is "Function" and it may be customized using the Qualys user interface.
ud3={attribute3}	(Optional) Specify a value for the user-defined host attribute 3. Initially the name of this attribute is "Asset Tag" and it may be customized using the Qualys user interface.
comment={text}	(Optional) Specify comments, notes about the target host IP addresses. The comments may include a maximum of 2048 characters (ascii). A specified comment overwrites any existing comment.

Examples

(Manager) Use this URL to add the IP addresses "10.10.10.1-10.10.10.255", tracked by IP address, to the subscription:

```
https://qualysapi.qualys.com/msp/asset_ip.php?action=add&
host_ips=10.10.10.1-10.10.10.255&owner=acme_bb&ud1=Toyko
&ud2=Manufacturing&ud3=4567
```

Next we'll describe some use cases for a user account including several IP addresses that have been scanned. Multiple host scan data entries are shown below.

	IP Address	NetBIOS Host name	DNS Host name	Tracking Method
1	10.10.10.1	Apple	corp1.acme.com	IP address
2	10.10.10.1	Orange	corp1.acme.com	IP address
3	64.41.134.60	DEMO02	demo02.qualys.com	NetBIOS host name

The host "10.10.10.1" in the user account has been scanned 2 times and there are 2 host scan data entries. For the first scan in row 1 the NetBIOS host name was detected as Apple, and for the second scan in row 2 the NetBIOS host name was detected as Orange.

Use this URL to add the comment "RB Team" to both host scan data entries:

```
https://qualysapi.qualys.com/msp/asset_ip.php?action=edit&
host_ips=10.10.10.1&comment=RB+Team
```

Use this URL to add the comment "RB Team" to the host scan data entry with the NetBIOS host name "Apple":

```
https://qualysapi.qualys.com/msp/asset_ip.php?action=edit&
host_ips=10.10.10.1&comment=RB+Team&host_netbios=Apple
```

It's not possible to change the tracking method for IP address "10.10.10.1" in the sample user account because there are 2 host scan data entries with different NetBIOS host names. Note that this limitation applies when there are multiple host scan data entries with different DNS names. For this user account, the URL below will return an error:

```
https://qualysapi.qualys.com/msp/asset_ip.php?action=edit&
host_ips=10.10.10.1&tracking_method=netbios
```

To resolve the error, log into the Qualys user interface and edit the host and follow the online instructions to purge host scan data entries. If you select the purge option, the most recent scan data is saved and the older scan data is purged (removed from the user account).

The IP address "64.41.134.60" has only one host scan data entry, so you can change the tracking method. Use this URL to change the tracking method from NetBIOS host name to DNS host name:

```
https://qualysapi.qualys.com/msp/asset_ip.php?action=edit&
host_ips=64.41.134.60&tracking_method=dns
```

XML Status Report

After processing an asset IP update, the **`asset_ip.php`** function returns an XML status message like this:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE GENERIC_RETURN SYSTEM
"https://qualysapi.qualys.com/generic_return.dtd">
<GENERIC_RETURN>
  <API name="asset_ip.php" username="mycompany_jb" at="2006-03-
20T11:14:28Z" />
  <RETURN status="SUCCESS">
     The operation was successfully completed.
  </RETURN>
</GENERIC_RETURN>
```

The DTD for the XML status message can be found at the following URL:

```
https://qualysapi.qualys.com/generic_return.dtd
```

View Asset IP List

asset_ip_list.php Function

The Asset IP List API (**/msp/asset_ip_list.php**) is used to view a list of asset IP addresses in the user account. To view the asset IP list, use the following URL:

```
https://qualysapi.qualys.com/msp/asset_ip_list.php
```

Express Lite: This API is available to Express Lite users.

When no parameters are specified with an **asset_ip_list.php** request, the function returns a list of IP ranges. Each range is defined by a start IP address and an end IP address. For an individual IP address not in a range, the IP address is returned in its own range where the start and end IPs are the same.

Optional parameters allow you to retrieve additional host details about hosts that have been scanned and hosts that have not been scanned. When **detailed_results=1** is specified, the report includes details for scanned hosts sorted by IP address. Details for these hosts appear under the <RESULTS> element. Included are scanned hosts with vulnerabilities detected, as well as scanned hosts with no vulnerabilities detected. Specifically, the details provided for each host include the tracking method, the DNS host name when known, the NetBIOS host name when known, the operating system detected, and user-supplied configurations such as the asset owner, comments, and parameters.

When **detailed_no_results=1** is specified, the report includes details for hosts that do not have associated assessment (scan) data. Details for these hosts appear under the <NO_RESULTS> element. Assessment data is part of a host's vulnerability history, which is saved separately from saved scan results. Hosts without assessment data include hosts that have not been scanned, hosts that were scan targets and were identified as not alive during host discovery (and thus not scanned), and hosts that were scanned and then purged. When this option is set, details are sorted by host tracking method, comment, owner, and user-defined parameters.

The **detailed_results** parameter and **detailed_no_results** parameter may be specified together in the same **asset_ip_list.php** request. When specified together, the IP list report includes details for all hosts in the user account. Each host will appear under <RESULTS> or <NO_RESULTS>.

User permissions for the **asset_ip_list.php** function are described below.

User Role	Permissions
Manager	View all IP addresses in subscription.
Unit Manager	View IP addresses in user's business unit.
Scanner	View IP addresses in user's account.
Reader	View IP addresses in user's account.

Parameters

The parameters for **asset_ip_list.php** are described below. These parameters are optional, and are used to retrieve host details. Both parameters may be specified together in the same **asset_ip_list.php** request to retrieve host details for all hosts in the user account.

Parameter	Description
detailed_results={0|1}	(Optional) Specifies whether to display details for scanned hosts, sorted by IP address. These include hosts with vulnerabilities detected, and hosts with no vulnerabilities detected. By default, details are not displayed for scanned hosts. To display details for scanned hosts, specify **detailed_results=1**.
detailed_no_results={0|1}	(Optional) Specifies whether to display details for hosts without assessment (scan) data. These include hosts that have not been scanned, hosts that were scan targets but were found not alive during host discovery, and hosts purged by users. These details are sorted by host tracking method, comment, owner, and user-defined parameters. By default, details are not displayed for hosts without assessment data. To display these details, specify **detailed_no_results=1**.

XML Report

The DTD for the XML IP list report returned by the **asset_ip_list.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/ip_list.dtd
```

Appendix D provides information about the XML report generated by the **asset_ip_list.php** function, including a recent DTD and XPath listing.

Add/Edit Domains

asset_domain.php Function

The Asset Domain API (**/msp/asset_domain.php**) is used to manage (add and edit) asset domains and related netblocks in the subscription. The domains in the subscription may be used as targets for network discovery, also referred to as mapping. For information on domains with netblocks, refer to "Using Domains with Netblocks" in Chapter 3. Using the Qualys user interface, Managers can assign domains to other users.

Express Lite: This API is available to Express Lite users.

The **asset_domain.php** function enables a Manager to make a request to add or edit domains in the subscription. When you make a request, the function performs the requested update and returns an XML document indicating the status of the request.

User permissions for the **asset_domain.php** function are described below.

User Role	Permissions
Manager	Add/Edit asset domains and related netblocks in the subscription.
Unit Manager	No permission to add/edit domains and related netblocks.
Scanner	No permission to add/edit domains and related netblocks.
Reader	No permission to add/edit domains and related netblocks.

Parameters

The parameters for **asset_domain.php** are described below.

Parameter	Description
action=add | edit	(Required) A flag indicating an add or edit request. Specify "add" to add a new domain, or "edit" to edit an existing domain.
domain={domain}	(Required) Specifies the domain name to add or edit. Include the domain name only; do not enter "www." at the start of the domain name.
netblock={ranges}	(Optional for add request, and Required for an edit request) Specifies the netblock(s) associated with the domain name. Multiple netblocks are comma separated. For an edit request, it's not possible to add or remove netblocks for a domain. To clear associated netblocks for an existing domain, specify **netblock=**

Examples

Add Domain

Use the URL below to add the domain "mydomain.com" to the subscription:

```
https://qualysapi.qualys.com/msp/asset_domain.php?action=add&
domain=mydomain.com
```

Use the URL below to add the domain "mydomain.com" with netblocks to the subscription:

```
https://qualysapi.qualys.com/msp/asset_domain.php?action=add&
domain=mydomain.com&netblock=10.10.10.0/24,10.2.34.44-
10.2.34.49
```

Use the URL below to add the domain "none" with netblocks to the subscription:

```
https://qualysapi.qualys.com/msp/asset_domain.php?action=add&
domain=none&netblock=10.10.10.0/24,64.41.134.59-64.41.134.61
```

Edit Domain

For the domain "acme.com" there are no netblocks defined. Use the URL below to add netblocks to the domain:

```
https://qualysapi.qualys.com/msp/asset_domain.php?action=edit&
domain=acme.com&netblock=10.10.10.0/24,10.1.1.0-10.1.1.100
```

For the domain "mycompany.com" there are multiple netblocks defined. Use the URL below to remove all netblocks associated with the domain:

```
https://qualysapi.qualys.com/msp/asset_domain.php?action=edit&
domain=mycompany.com&netblock=
```

XML Status Report

After processing an asset domain update, the **asset_domain.php** function returns an XML status message like this:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE GENERIC_RETURN SYSTEM
"https://qualysapi.qualys.com/generic_return.dtd">
<GENERIC_RETURN>
  <API name="asset_domain.php" username="mycompany_jb"
at="2006-03-20T11:14:28Z" />
  <RETURN status="SUCCESS">
     The operation was successfully completed.
  </RETURN>
</GENERIC_RETURN>
```

The DTD for the XML status message can be found at the following URL:

```
https://qualysapi.qualys.com/generic_return.dtd
```

View Asset Domain List

asset_domain_list.php Function

The **asset_domain_list.php** function is used to view a list of asset domains in the user account. To view the asset domain list, use the following URL:

```
https://qualysapi.qualys.com/msp/asset_domain_list.php
```

User permissions for the **asset_domain_list.php** function are described below.

User Role	Permissions
Manager	View all domains in subscription.
Unit Manager	View domains in user's business unit.
Scanner	View domains in user's account.
Reader	View domains in user's account.

XML Report

The DTD for the XML domain list report returned by the **asset_domain_list.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/domain_list.dtd
```

Appendix D provides information about the XML report generated by the **asset_domain_list.php** function, including a recent DTD and XPath listing.

Add/Edit Asset Group

asset_group.php Function

Function Overview

The Asset Group API (/msp/**asset_group.php**) is used to manage asset groups and related data, including IP addresses, domain names, scanner appliances, business information and CVSS Environmental metrics used to calculate CVSS scores (when the CVSS Scoring feature is enabled). Using asset groups you can prioritize assets and manage business risk. Asset groups provide great flexibility in managing cases where assets in a subscription have multiple business uses, possibly even different priorities, when part of multiple applications and/or business units.

Express Lite: This API is available to Express Lite users.

When you make a request using this API, our service performs the requested update and returns an XML document indicating the status of the request.

Asset Group Requests

A single request using the **asset_group.php** function allows you to add an asset group or edit an existing asset group. The asset group title, specified in the **title** parameter, is used to identify the asset group and is required for all requests. The **asset_group.php** function has several optional parameters for assigning asset group properties.

IPs, Domains, Scanner Appliances. An **asset_group.php** request allows the user to add or edit parameters for scanning, such as IP addresses, domain names, and scanner appliances. The user has permission to add or edit these assets only when they are available in the user account. For reference, the Qualys API provides information on the assets in the user account.

Function	Description
asset_ip_list.php	Returns a list of IP addresses and related information, such as tracking method, owner, user defined information, and user-defined parameters. For more information, see "View Asset IP List" earlier in this chapter.
asset_domain_list.php	Returns a list of domain names and related netblocks. For more information, see "View Asset Domain List" earlier in this chapter.
iscanner_list.php	Returns a list of scanner appliances. For more information, see "View Scanner Appliance List" in Chapter 4.

Edit Title. When editing an asset group, the title can be changed using the **new_title** parameter. For this type of request, you specify both the **title** parameter and the **new_title** parameter in the edit request.

Edit IP Addresses. For an add request, specify the **host_ips** parameter to add IPs. If you specify this parameter for an edit request, the IPs you specify replace any existing IPs. For example, if the target asset group includes IP 10.10.10.1 and the edit request includes the parameter **host_ips=10.10.10.20**, then IP 10.10.10.20 is saved in the asset group and IP 10.10.10.1 is removed. Other parameters are available for an edit request, allowing you to manage IP addresses on an ongoing basis. The **add_host_ips** parameter allows you to append IP addresses in an existing group, and the **remove_host_ips** parameter allows you to remove IP addresses in an existing group. (Note if both **add_host_ips** and **remove_host_ips** are included in the same request, the IPs in **add_host_ips** are added first before IPs in **remove_host_ips** are removed.)

Edit Other Attributes. When editing asset group attributes other than title or IP addresses, as described above, existing attribute values are replaced with newly specified values.

Clear Attributes. When editing asset group attributes other than "title", the user can send an edit request to clear (reset) attributes by assigning the empty string "". For example, if the "division" attribute is set to "Division 70" and you want to clear the division value, send an edit request with division equal to empty string (division="").

CVSS Scoring Attributes

CVSS stands for the Common Vulnerability Scoring System, the emerging open standard for vulnerability scoring. CVSS scoring provides a common language for understanding vulnerabilities and threats.

When CVSS Scoring is enabled in your account, you can assign CVSS Environmental metrics to an asset group. These metrics are used to calculate the final CVSS scores for vulnerabilities in automatic scan reports, when the reports have target asset groups.

User Permissions

User permissions for the **asset_group.php** function are described below. Unit Managers and Scanners have edit permissions on limited asset groups related to asset group owner (user account). Note the user who creates an asset group becomes its owner.

User Role	Permissions
Manager	Add/Edit asset group in subscription. Asset group may include IP addresses, domains, and scanner appliances in the subscription.
Unit Manager	Add/Edit asset group in user's business unit. Asset group may include IP addresses, domains, and scanner appliances in the user's business unit. Edit asset group owned by any user (self, another Unit Manager, Scanner) in the same business unit.
Scanner	Add/Edit asset group in user's business unit. Asset group may include IP addresses, domains, and scanner appliances in the user's account. Edit asset group owned by the user.
Reader	No permission to add/edit an asset group.

Parameters

The parameters for **asset_group.php** are described below.

Parameter	Description
action=add|edit	(Required) A flag indicating an add or edit request. Specify "add" to add a new asset group, or "edit" to edit an existing group.
title={title}	(Required) Specifies the title of the asset group. The title may include a maximum of 255 characters (ascii).
new_title={new_title}	(Optional for edit request only) Specifies the new title of the asset group. The title may include a maximum of 255 characters (ascii). This parameter may be specified for an edit request (and it is invalid for an add request).

Parameter	Description
host_ips={addresses}	(Optional) Specifies one or more IP addresses to be added to the asset group. This parameter may be specified for an add request (**action=add**) or edit request (**action=edit**). When this parameter is specified for an edit request, IPs you specify are added and any existing IPs are removed. You may enter a combination of IPs and IP ranges. Multiple entries are comma separated. For more information on entering target IPs and ranges, see "Target Hosts" in Chapter 2.
	This parameter and the **add_host_ips** parameter or the **remove_host_ips** parameter cannot be specified in the same request.
add_host_ips={addresses}	(Optional) Specifies one or more IP addresses to be added to the existing asset group. This parameter may be specified for an edit request (**action=edit**). You may enter a combination of IPs and IP ranges. Multiple entries are comma separated. For more information on entering target IPs and ranges, see "Target Hosts" in Chapter 2.
	This parameter and the **host_ips** parameter cannot be specified in the same request.
remove_host_ips={addresses}	(Optional) Specifies one or more IP addresses to be removed from the existing asset group. This parameter may be specified for an edit request (**action=edit**). You may enter a combination of IPs and IP ranges. Multiple entries are comma separated. For more information on entering target IPs and ranges, see "Target Hosts" in Chapter 2.
	This parameter and the **host_ips** parameter cannot be specified in the same request.
domains={domains}	(Optional) Specifies one or more domains to be added to the asset group. Each domain entry may include one or more netblocks (IP ranges). Multiple domain entries are comma separated. Multiple netblock entries are semi-colon separated. For more information on entering domains, see "Target Domains" in Chapter 3.

Parameter	Description
scanner_appliances={name1,name2...}	(Optional) Specifies the names of the scanner appliances to be added to the asset group. Multiple appliance names are comma separated. For more information, see "Scanner Selection for Scans" in Chapter 2 and "Scanner Selection for Maps" in Chapter 3.
default_scanner_appliance={name}	(Optional) Specifies the name of the default scanner appliance for the asset group. The default scanner appliance name must be available in the user account, and must be one of the appliance names in the asset group. A default scanner must be defined for an asset group with scanner appliances. This parameter must be specified when adding a group with appliances.
business_impact={level}	(Optional) Specifies the business impact level, or business risk, of the assets (IP addresses) in the asset group. The impact level value is case sensitive. When adding a new asset group, the default is set to the rank 4 value, which is initially set to High. The impact level is used to calculate business risk in scan reports using automatic data selection. The higher the impact level, the higher the potential for business loss if compromised. The impact level is defined in the Qualys user interface. Initial impact levels are provided by Qualys. When Qualys provided levels are used, a valid value is: Critical (rank 5), High (rank 4), Medium (rank 3), Minor (rank 2), or Low (rank 1).
division={value}	(Optional) The division name or organization that the assets belong to. The division may include a maximum of 64 characters (ascii).
function={value}	(Optional) The user-defined business function of the assets (IP addresses) in the asset group. The function may include a maximum of 64 characters (ascii).
location={value}	(Optional) The user-defined location where the assets in the asset group are located. The location may include a maximum of 64 characters (ascii).
comments={value}	(Optional) The user-defined notes about the asset group. The comment section may include a maximum of 255 characters (ascii).

Parameter	Description
cvss_enviro_cdp={setting}	(Optional) The setting for CVSS Environmental metric: Collateral Damage Potential. This parameter is valid only when CVSS Scoring is enabled in the user account. A valid value is: none, low, low-medium, medium-high, or high. When adding a new asset group, the default value is not defined.
cvss_enviro_td={setting}	(Optional) The setting for CVSS Environmental metric: Target Distribution. This parameter is valid only when CVSS Scoring is enabled in the user account. A valid value is: none, low, medium, or high. When adding a new asset group, the default value is not defined.
cvss_enviro_cr={setting}	(Optional) The setting for CVSS Environmental metric: Confidentiality Requirement. This parameter is valid only when CVSS Scoring is enabled in the user account. A valid value is: low, medium, or high. When adding a new asset group, the default value is not defined.
cvss_enviro_ir={setting}	(Optional) The setting for CVSS Environmental metric: Integrity Requirement. This parameter is valid only when CVSS Scoring is enabled in the user account. A valid value is: low, medium, or high. When adding a new asset group, the default value is not defined.
cvss_enviro_ar={setting}	(Optional) The setting for CVSS Environmental metric: Availability Requirement. This parameter is valid only when CVSS Scoring is enabled in the user account. A valid value is: low, medium, or high. When adding a new asset group, the default value is not defined.
network_id={value}	(Optional) This parameter is valid only when the network support feature is enabled for your account and the request includes action=add. Want to assign your new asset group to a custom network? Specify a network ID for the custom network - this must already be defined in your account. If you have the network support feature enabled, we'll assign the Global Default Network (network_id=0) by default.

Examples

The URL below adds a new asset group "Finance" for scanning that includes internal IP addresses and scanner appliances:

```
https://qualysapi.qualys.com/msp/asset_group.php?action=add&
title=Finance&host_ips=10.10.10.1-10.10.10.255&scanner_appli
ances=Tiger,Monkey&default_scanner_appliance=Tiger
```

The URL below edits the asset group "Finance" and renames the title to "Finance NY":

```
https://qualysapi.qualys.com/msp/asset_group.php?action=edit&
title=Finance&new_title=Finance+NY
```

The URL below edits the asset group "Finance" and appends the IPs 10.10.10.1-10.10.10.100 and 64.41.134.60 to the group:

```
https://qualysapi.qualys.com/msp/asset_group.php?action=edit&
title=Finance&add_host_ips=10.10.10.110.10.10.100,64.41.134.60
```

The URL below adds a new asset group "Finance NY Map" that includes domain names for network discovery/mapping:

```
https://qualysapi.qualys.com/msp/asset_group.php?action=add&
title=Finance+NY+Map&domains=mycompany.com,none:10.10.10.1-
10.10.10.255,qualys-test.com&scanner_appliances=Tiger&defau
lt_scanner_appliance=Tiger
```

The URL below adds a new asset group "Finance" for scanning that includes internal IP addresses and scanner appliances, and CVSS Environmental metrics are assigned:

```
https://qualysapi.qualys.com/msp/asset_group.php?action=add&
title=Finance&
host_ips=10.10.10.1-10.10.10.255&
scanner_appliances=Tiger,Monkey&
default_scanner_appliance=Tiger&
cvss_enviro_cdp=medium-high&
cvss_enviro_td=medium&
cvss_enviro_ir=medium&
cvss_enviro_ar=high
```

The URL below edits the asset group "Finance" and changes the CVSS Environmental metric Integrity Requirement to "low".

```
https://qualysapi.qualys.com/msp/asset_group.php?action=edit&
title=Finance&cvss_enviro_ir=low
```

XML Status Report

After processing an asset group update, the **asset_group.php** function returns an XML status message like this:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE GENERIC_RETURN SYSTEM
"https://qualysapi.qualys.com/generic_return.dtd">
<GENERIC_RETURN>
  <API name="asset_group.php" username="mycompany_jb" at="2006-
03-20T11:14:28Z" />

  <RETURN status="SUCCESS">
     The operation was successfully completed.
  </RETURN>
</GENERIC_RETURN>
```

The DTD for the XML status message can be found at the following URL:

```
https://qualysapi.qualys.com/generic_return.dtd
```

View Asset Group List

asset_group_list.php Function

The Asset Group List API (/msp/**asset_group_list.php)**is used to view the asset groups in the user account. To view the asset groups in the user account, use the following URL:

```
https://qualysapi.qualys.com/msp/asset_group_list.php
```

Express Lite: This API is available to Express Lite users.

The XML results returned by the **asset_group_list.php** function provide details about each asset group, such as its title, ID, associated IPs, domains, scanner appliances, and user-defined business information. CVSS scoring metrics are listed when the CVSS Scoring feature is enabled in the user account. See "CVSS Scoring Attributes".

The **title** parameter (optional) is used to request information on a specific asset group. To view an asset group with the title "Worldwide Sales", use the following URL:

```
https://qualysapi.qualys.com/msp/asset_group_list.php?
title=Worldwide+Sales
```

User permissions for the **asset_group_list.php** function are described below.

User Role	Permissions
Manager	View asset groups in the subscription.
Unit Manager	View asset groups in the user's business unit. Ability to view asset groups assigned to the business unit, and asset groups owned by any user (self, another Unit Manager, Scanner) in the same business unit.
Scanner	View asset groups in the user's account. Ability to view asset groups assigned to the user, and asset groups owned by the user.
Reader	View asset groups in the user's account. Ability to view asset groups assigned to the user.

XML Report

The DTD for the XML asset group list returned by the **asset_group_list.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/asset_group_list.dtd
```

Appendix D provides information about the XML report generated by the **asset_group_list.php** function, including a recent DTD and XPath listing

Delete Asset Group

asset_group_delete.php Function

The Asset Group Delete API (**/msp/asset_group_delete.php**) is used to delete an asset group from the user account. To delete an asset group from the user account, use the following URL (where **title={title}** represents the asset group title):

```
https://qualysapi.qualys.com/msp/asset_group_delete.php?
title={title}
```

Express Lite: This API is available to Express Lite users.

User permissions for the **asset_group_delete.php** function are described below.

User Role	Permissions
Manager	Delete any asset group in the subscription.
Unit Manager	Delete asset group owned by any user (self, another Unit Manager, Scanner) in the same business unit.
Scanner	Delete asset group owned by the user.
Reader	No permission to delete an asset group.

XML Status Report

After processing an asset group update, the **asset_group_delete.php** function returns an XML status message like this:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE GENERIC_RETURN SYSTEM
"https://qualysapi.qualys.com/generic_return.dtd">
<GENERIC_RETURN>
  <API name="asset_group_delete.php" username="mycompany_jb"
at="2006-03-20T11:14:28Z" />
  <RETURN status="SUCCESS">
     The operation was successfully completed. Please note that
some of your scheduled tasks may become inactive.
  </RETURN>
</GENERIC_RETURN>
```

The DTD for the XML status message can be found at the following URL:

```
https://qualysapi.qualys.com/generic_return.dtd
```

Search Assets by Attributes

asset_search.php Function

The **asset_search.php** function is used to search assets in the user account and retrieve asset information matching search attributes. For the search target, you may specify a combination of IP addresses, asset groups, a DNS host name and/or a NetBIOS host name. Several search attributes are available to refine the search results, such as operating system, running services, open ports, QIDs (Qualys vulnerability IDs) and last scan date.

The XML search results returned by the **asset_search.php** function include host scan data for the target hosts. Hosts must be scanned at least once to appear in asset search results. If a host was scanned and then purged, the host does not appear in asset search results until after the host is scanned again. Disabled vulnerabilities and Ignored vulnerabilities, as defined in the Qualys user interface, are not included in the XML results.

The XML results include a header section and a results section. The header section contains information about the user requesting the report, the date of the request, and the search criteria. The results section contains a list of host records, each of which includes host properties. The properties returned depend on what information is available in the user account and which search attributes were specified. The IP address and tracking method are always reported. Ports and services are reported if they were among the search criteria. Other properties are returned when available for the host.

If scan tasks do not scan for certain vulnerabilities, then the appropriate host scan data may not be available for searching. Specifically, these vulnerability checks must be scanned.

Host Scan Data to Search	Vulnerability Check
Operating System	"Operating System Detected" vulnerability check (QID 45017)
TCP services	"Open TCP Services List" vulnerability check (QID 82023)
UDP services	"Open UDP Services List" vulnerability check (QID 82004)

When host scan data is not available for searching, any search requests on the data return no asset search results. For example, if you performed a selective vulnerability scan on a particular host without scanning for the "Operating System Detected" vulnerability check (QID 45017), and then send an **asset_search.php** request for hosts by operating system, using the **host_os** parameter, this particular host is not searched and it will not appear in scan results.

User permissions for the **asset_search.php** function are described below.

User Role	Permissions
Manager	Search all IP addresses in the subscription.
Unit Manager	Search IP addresses in the user's business unit.
Scanner	Search IP addresses in the user's account.
Reader	Search IP addresses in the user's account.

Parameters

The parameters for **asset_search.php** are described below. At least one parameter is required to identify target hosts.

Target Hosts

The search target identifies target hosts. You must specify **target_ips** with IP addresses/ranges and/or **target_asset_groups** with asset group titles. All specified hosts are searched and results are returned for hosts matching the host parameters given.

Parameter	Description
target_ips={addresses}	(Optional) For the search target, specify hosts based on one or more IP addresses. Enter IP addresses and/or ranges to be included. Multiple entries are comma separated. For more information, see "Target Hosts" in Chapter 2.
	One of these parameters must be specified: **target_ips** or **target_asset_groups**.
target_asset_groups={title1,title2,...}	(Optional) For the search target, specify hosts in one or more asset groups. Enter one or more asset group titles to be included. Multiple titles are comma separated. The title "All" may be specified to include all IP addresses in the user account.
	One of these parameters must be specified: **target_ips** or **target_asset_groups**.

Host Parameters

Specifying host parameters allows you to limit search results to hosts having certain attributes. Attributes include operating system, open ports, running services and others. When host parameters are specified, only hosts in the search target with the specified attributes are returned.

Parameter	Description
dns={prefix:text}	(Optional) Search for hosts based on a DNS host name that matches a string you specify. A valid prefix is: begin, match, contain, or end. The host name string may have a maximum of 256 characters.
netbios={prefix:text}	(Optional) Search for hosts based on a NetBIOS host name that matches a string you specify. A valid prefix is: begin, match, contain, or end. The host name string may have a maximum of 256 characters.
host_os={prefix:text}	(Optional) Search for hosts with an operating system name using a text match prefix. For example, to search for operating system names containing Linux, specify this: **`host_os=contain:Linux`** A valid prefix is: begin, match, contain, or end. A valid operating system name must match a Qualys defined name which the scanning engine has already scanned and detected in the subscription. Operating system names are case sensitive. An operating system name may include a maximum of 128 characters.
tracking_method={method}	(Optional) Search for hosts with a particular tracking method. A valid value is: “ip” (for IP tracked hosts), “dns” (for DNS tracked hosts), or “netbios” (for NetBIOS tracked hosts).
vuln_service={service}	(Optional) Search for hosts running particular service names. Up to 10 service names may be entered. Multiple services are comma separated. A valid service name must match a Qualys defined name. The service name may include a maximum of 128 characters.
vuln_port={number}	(Optional) Search for hosts with particular open ports (TCP and UDP). Up to 10 port numbers may be entered. Multiple ports are comma separated. A port number may include a maximum of 5 characters.

Parameter	Description
vuln_qid={qid}	(Optional) Specifies one or more QIDs (Qualys IDs) to search for hosts with particular vulnerabilities. Up to 20 QIDs may be entered. Multiple QIDs are comma separated. A QID entry may include a maximum of 6 characters.
vuln_results={prefix:text}	(Optional) This parameter is valid only when specified with the **`vuln_qid`** parameter. Search for hosts with QIDs containing certain vulnerability results using a text match prefix. For example, to search for results text starting with SQL, specify this: **`vuln_results=begin:SQL`** A valid prefix is: begin, match, contain, or end. A vulnerability results entry may include a maximum of 256 characters.
last_scan={prefix:n_days}	(Optional) Search for hosts that were last scanned in a time frame using a match prefix. For example, to search for hosts last scanned within 15 days, specify this: **`last_scan=within:15`** A valid prefix is: “within” or “not_within”. The number of days is an integer from 1 to 365.

Examples

The URL below searches for hosts in the asset group "Critical Servers" that are vulnerable to QID 27279 "FTP Backdoor Allows Administrator Privileges":

```
https://qualysapi.qualys.com/msp/asset_search.php?target_asset_
groups=Critical+Servers&vuln_qid=27279
```

The URL below searches for hosts in the asset group "Critical Servers" that have vulnerabilities on TCP ports 80 and 443:

```
https://qualysapi.qualys.com/msp/asset_search.php?
target_asset_groups=Critical+Servers&vuln_port=80,443
```

The URL below searches for hosts in the IP range "10.10.10.1-10.10.10.255" that were scanned within the last 10 days:

```
https://qualysapi.qualys.com/msp/asset_search.php?
target_ips=10.10.10.1-10.10.10.255&last_scan=within:10
```

The URL below searches for hosts which have a DNS host name starting with the string "demo":

```
https://qualysapi.qualys.com/msp/asset_search.php?
target_asset_groups=All&dns=begin:demo
```

XML Report

The DTD for the XML asset search results returned by the **`asset_search.php`** function can be found at the following URL:

```
https://qualysapi.qualys.com/asset_search_report.dtd
```

Appendix D provides information about the XML report generated by the **`asset_search.php`** function, including a recent DTD and XPath listing.

Download Asset Data Report

asset_data_report.php Function

The **asset_data_report.php** function is used to download an asset data report based on a scan report template (automatic) in the user account. Parameters allow for downloading an asset data report by template title or template ID. The XML report returned by this function includes detailed information on each host based on the most up-to-date vulnerability data. Disabled vulnerabilities and Ignored vulnerabilities are not included in the XML report.

Using the **asset_data_report.php** function, you can download a scan report with current vulnerability data using an automatic type scan report template. It's not possible to download scan report using a manual report template or a system report template like the Qualys Top 20 Report. The **report_template_list.php** function provides a list of available report templates available in your account.

The report target is defined in the report template itself. The target may include a combination of IP addresses, ranges and asset groups.

The **template_title** parameter is used to request an asset data report based on a scan report template title. To download a report for the template "Technical Report", use the following URL:

```
https://qualysapi.qualys.com/msp/asset_data_report.php?
template_title=Technical+Report
```

The **template_id** parameter is used to request an asset data report based on template ID for an automatic type scan report To download a report for template ID "13527", use the following URL:

```
https://qualysapi.qualys.com/msp/asset_data_report.php?
template_id=13527
```

User permissions for the **asset_data_report.php** function are described below.

User Role	Permissions
Manager	Download asset data report for IP addresses in subscription.
Unit Manager	Download asset data report for IP addresses in user's business unit.
Scanner	Download asset data report for IP addresses in user's account.
Reader	Download asset data report for IP addresses in user's account.

Report Template List

The **report_template_list.php** function provides a list of available report templates, including template titles and IDs, in the user account. The report list includes templates for all report types.

To retrieve a list of report templates, use this URL:

```
https://qualysapi.qualys.com/msp/report_template_list.php
```

The DTD for the XML document returned from **report_template_list.php** can be found at the following URL:

```
https://qualysapi.qualys.com/report_template_list.dtd
```

Sample report template list output is shown below:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORT_TEMPLATE_LIST SYSTEM
"https://qualysapi.qualys.com/report_template_list.dtd">
<REPORT_TEMPLATE_LIST>
  <REPORT_TEMPLATE>
    <ID>235288</ID>
    <TYPE>Auto</TYPE>
    <TEMPLATE_TYPE>Scan</TEMPLATE_TYPE>
    <TITLE><![CDATA[Windows Authentication QIDs]]></TITLE>
    <USER>
      <LOGIN><![CDATA[quays_ak12]]></LOGIN>
      <FIRSTNAME><![CDATA[Jason]]></FIRSTNAME>
      <LASTNAME><![CDATA[Kim]]></LASTNAME>
    </USER>
    <LAST_UPDATE>2008-12-12T18:09:10Z</LAST_UPDATE>
    <GLOBAL>0</GLOBAL>
  </REPORT_TEMPLATE>
  <REPORT_TEMPLATE>
    <ID>235164</ID>
    <TYPE>Auto</TYPE>
    <TEMPLATE_TYPE>Policy</TEMPLATE_TYPE>
    <TITLE><![CDATA[My Policy Report Template]]></TITLE>
    <USER>
      <LOGIN><![CDATA[quays_vs]]></LOGIN>
      <FIRSTNAME><![CDATA[Victor]]></FIRSTNAME>
      <LASTNAME><![CDATA[Smith]]></LASTNAME>
    </USER>
    <LAST_UPDATE>2008-12-09T22:47:58Z</LAST_UPDATE>
```

```
    <GLOBAL>0</GLOBAL>
  </REPORT_TEMPLATE>
  <REPORT_TEMPLATE>
    <ID>232556</ID>
    <TYPE>Auto</TYPE>
    <TEMPLATE_TYPE>Scan</TEMPLATE_TYPE>
    <TITLE><![CDATA[Executive Report]]></TITLE>
    <USER>
      <LOGIN><![CDATA[quays_ak12]]></LOGIN>
      <FIRSTNAME><![CDATA[Jason]]></FIRSTNAME>
      <LASTNAME><![CDATA[Kim]]></LASTNAME>
    </USER>
    <LAST_UPDATE>2008-11-11T17:11:55Z</LAST_UPDATE>
    <GLOBAL>1</GLOBAL>
  </REPORT_TEMPLATE>
  <REPORT_TEMPLATE>
    <ID>232557</ID>
    <TYPE>Auto</TYPE>
    <TEMPLATE_TYPE>Scan</TEMPLATE_TYPE>
    <TITLE><![CDATA[Technical Report]]></TITLE>
    <USER>
      <LOGIN><![CDATA[quays_ak12]]></LOGIN>
      <FIRSTNAME><![CDATA[Jason]]></FIRSTNAME>
      <LASTNAME><![CDATA[Kim]]></LASTNAME>
    </USER>
    <LAST_UPDATE>2008-11-11T17:11:55Z</LAST_UPDATE>
    <GLOBAL>1</GLOBAL>
  </REPORT_TEMPLATE>
...
</REPORT_TEMPLATE_LIST>
```

Each <REPORT_TEMPLATE> element identifies template properties, including the ID and title, in the sub-elements described below.

Element	Description
<ID>	The template ID number.
<TYPE>	The template type: Auto (for automatic) or Manual. Note: The **asset_data_report.php** function can be used to download a scan report using an automatic template.
<TEMPLATE_TYPE>	The report template type: — Scan (for a scan report template) — Map (for a map report template) — Remediation (for a remediation report template) — Compliance (for a compliance report template) — Policy (for a compliance policy report template) — Patch (for a patch report template)
<TITLE>	The template title, as defined in the Qualys user interface.
<USER>	The template owner, identified by login, first name and last name. For a system template, the login "system" is reported. Note: The **asset_data_report.php** function cannot be used to download a report using a system template.
<LAST_UPDATE>	The most recent date and time when the template was updated.
<GLOBAL>	For a global template, the value 1 appears. For a non global template, the value 0 appears.

XML Report

The DTD for the XML report returned by the **asset_data_report.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/asset_data_report.dtd
```

Appendix D provides information about the XML report generated by the **asset_data_report.php** function, including a recent DTD and XPath listing.

Download Asset Range Info Report

asset_range_info.php Function

The **asset_range_info.php** function is used to download an asset report for a range of IP addresses specified with the request. The report target may include a combination of IP addresses, ranges and asset groups. The XML report returned by this function includes detailed information on each host based on the most up-to-date vulnerability data. Disabled vulnerabilities and Ignored vulnerabilities, as defined in the Qualys user interface, are not included in the XML report.

This report is based on a Qualys defined report template. For more information, see "Pre-defined Template for XML Report"

User permissions for the **asset_range_info.php** function are described below.

User Role	Permissions
Manager	Download asset range info report for IP addresses and asset groups in subscription.
Unit Manager	Download asset range info report for IP addresses and asset groups in user's business unit.
Scanner	Download asset range info report for IP addresses and asset groups in user's account.
Reader	Download asset range info report for IP addresses and asset groups in user's account.

Parameters

The parameters for **asset_range_info.php** are described below.

Parameter	Description
target_ips={addresses}	(Optional) Specifies one or more IP addresses and/or ranges to be included in the report target. Multiple entries are comma separated. The report target may include a combination of IP addresses, ranges, and asset groups. For more information on syntax, see "Target Hosts" in Chapter 2. This parameter and/or the **target_asset_groups** parameter must be specified.

Parameter	Description
target_asset_groups={title1,title2,...}	(Optional) Specifies one or more asset group titles to be included in the report target. The asset group title "All" may be specified to include all IP addresses in the user account. Multiple titles are comma separated. The report target may include a combination of IP addresses, ranges, and asset groups. For more information on syntax, see "Target Hosts" in Chapter 2.
	This parameter and/or the **target_ips** parameter must be specified.

Examples

Use the following URL to download an asset range info report for the target IP address range "10.10.10.1-10.10.10.17" and "10.0.100.0/24" as well as the target IP addresses "10.10.10.52".

```
https://qualysapi.qualys.com/msp/asset_range_info.php?
target_ips=10.10.10.1-10.10.10.17,10.0.100.0/24,10.10.10.52
```

Use the following URL to download an asset range info report for the asset group with the title "New York":

```
https://qualysapi.qualys.com/msp/asset_range_info.php?
target_asset_groups=New+York
```

Use the following URL to download an asset range info report for the target IP address range "10.0.100.0/24" and the asset groups "New York" and "Tokyo":

```
https://qualysapi.qualys.com/msp/asset_range_info.php?
target_ips=10.0.100.0/24&target_asset_groups=New+York,Tokyo
```

XML Report

The DTD for the XML report returned by the **asset_range_info.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/asset_range_info.dtd
```

Appendix D provides information about the XML report generated by the **asset_range_info.php** function, including a recent DTD and XPath listing.

Pre-defined Template for XML Report

The asset range info report output is generated based on a Qualys defined report template, which cannot be configured by the API user. The settings directly correspond to report template settings in the Qualys user interface as described below.

Template setting	Description
Template Information	
Scan Results Selection Status	The template generates a status report using Automatic scan results selection. The service automatically gathers the most up-to-date scan results data based on report template settings.
Display Tab	
Report Summary Text Summary not checked	A text summary is not included for summary of vulnerabilities or detailed results.
Report Summary Graphics options not checked	Graphics are not included.
Detailed Results Sort by Host	Detailed results are sorted by host.
Detailed Results Vulnerability Details Options selected	Vulnerability details are included: Threat, Impact, Solution and Result.
Detailed Results Appendix selected	Report appendix is included.
Filter Tab	
Selective Vulnerability Reporting Complete selected	Complete KnowledgeBase (all vulnerabilities) is selected.
Filters Status Codes checked (except Fixed)	Vulnerabilities with these status codes are selected: New, Active, and Re-opened. (Note: Vulnerabilities with a status of Fixed are not included.)
Filters Severity Severity 1 to 5 selected	Vulnerabilities with all severity levels (1 to 5) are selected.
Filters Vulnerability Checks Active selected	All active vulnerability types are selected: vulnerabilities, potential vulnerabilities and information gathered.
Filters Vulnerability Checks Disabled not selected	Disabled vulnerabilities are not selected. This setting is not checked for vulnerabilities, potential vulnerabilities, and information gathered.

Template setting	Description
Filters Vulnerability Checks Ignored not selected	Ignored vulnerabilities are not selected. This setting is not checked for vulnerabilities and potential vulnerabilities (and does not apply to information gathered).
Included Categories All categories selected	All vulnerability categories are selected.
Services and Ports Tab	
Required Services none selected	No required services are selected.
Unauthorized Services none selected	No unauthorized services are selected.
Customizations	
customized vulnerabilites	Customized vulnerabilities are selected. This the default behavior of all Qualys scan report templates.

For complete information on report templates, refer to the Report section in the Qualys online help.

CHAPTER 6

Remediation Management

The Qualys API allows users to retrieve host information and ticket information for the purpose of remediation tracking and reporting in third-party applications.

This chapter describes remediation management using host information and remediation tickets in Qualys accounts. These topics are included:

- About Remediation Tickets
- Ticket Functions
  - Ticket Selection Parameters
  - View Ticket List
  - Edit Tickets
  - Delete Tickets
  - View Deleted Ticket List
  - Get Ticket Information
- Host Functions
  - View Host Information
  - Set Vulnerabilities to Ignore on Hosts

About Remediation Tickets

Qualys provides fully secure audit trails that track vulnerability status for all detected vulnerabilities. As follow up audits occur, vulnerability status levels — new, active, fixed, and re-opened — are updated automatically and identified in trend reports, giving users access to the most up-to-date security status. Using Remediation Workflow, Qualys automatically updates vulnerability status in remediation tickets, triggering ticket updates and closure in cases where vulnerabilities are verified as fixed.

Ticket Lifecycle

Qualys Manager users have the option to enable the Remediation Workflow feature for the subscription using the Qualys user interface. Remediation Workflow is an automated ticketing system based on remediation policy created by users. When this feature is enabled, new tickets are created automatically based on the user-defined policy.

Ticket updates occur automatically by the service, triggered by security audits, and by users editing tickets. Role-based access controls determine which users have the ability to view which tickets, ensuring that only the appropriate users can access ticket information. As new scan results become available, tickets are updated.

Users perform ticket updates when they take action on tickets by fixing vulnerabilities, adding comments, or reassigning to other users as appropriate. Users also have the ability to create tickets manually to track vulnerabilities which are not created automatically by the policy in place.

Ticket Information

A remediation ticket tracks a vulnerability detected on a particular host and port. Each ticket includes the following information:

- Properties — Every ticket is assigned a unique ticket number and ticket state (Open, Resolved, Closed/Fixed, Closed/Ignored). Tickets may have a designated assignee and may be marked as overdue or invalid.
- Host information — Host related information including IP address, operating system detected, DNS host name and NetBIOS host name (if applicable).
- Vulnerability information — Information about the vulnerability associated with this ticket, including the vulnerability title, its severity level as well as a description of the threat and a verified solution to fix the issue.
- History — Ticket history including a complete history of ticket actions.

With this information, users with access rights to the ticket may take action on the ticket to fix the vulnerability on the host.

Ticket Update Events

Several events trigger updates to remediation tickets. Some events occur as the result of users editing tickets and taking actions in the Qualys user interface, while others occur automatically by the service as the result of a scan. The table below describes how certain events cause ticket information to be updated.

Ticket Information	Ticket Update Event
New ticket	A new ticket was created. A ticket may be created by the service based on a policy rule and triggered by a scan. A ticket may be created by users for vulnerabilities that appear in their automatic scan reports.
Host information updated	The host information associated with the ticket was updated. This information may be updated by the service automatically based on new scan results. It is updated when users add host comments.
Host information purged (by a user)	The host information associated with the ticket was purged by a user. This permission is granted to all Managers automatically. Managers may grant this permission to Unit Managers, Scanners, and Readers.
Ticket statistics	The ticket statistics were updated by the service. Ticket statistics include the most recent date/time when the host was scanned, the first date/time when the host was scanned, and the number of times the vulnerability was detected on the host.
Ticket state/status (by the service)	An existing ticket may change state/status based on a scan. For example, if a scan verifies that a ticket's vulnerability is fixed, the ticket state is changed from Open to Closed/Fixed.
Ticket state/status (by a user)	An existing ticket may change state/status based on some user action. For example, a user can edit the ticket and change the state from Open to Resolved or Closed/Ignored.
Ticket assignee	The ticket was reassigned at least one time to a different user for remediation. Users can edit the ticket to reassign the ticket owner.
Ticket comments	Ticket comments were added by one or more users.
Vulnerability severity level	The vulnerability associated with the ticket was assigned a new severity level by a Manager user.
Vulnerability details	The vulnerability details for each vulnerability includes a description of the threat, impact, and solution. A Manager user may update these descriptions in the KnowledgeBase using the Qualys user interface.

Ticket Functions

A summary of the ticket functions that are available in the Qualys API are described below.

Function Name	Description
ticket_list.php	View a list of selected tickets which the API user has permission to access. Several methods for ticket selection are available. XML results returned using the ticket list output DTD: https://qualysapi.qualys.com/ticket_list_output.dtd
ticket_edit.php	Edit selected tickets in the subscription to update ticket state, change the assignee, and add comments. Several methods for ticket selection are available. Managers and Unit Managers have permission to run this function. XML results returned using the ticket edit output DTD: https://qualysapi.qualys.com/ticket_edit_output.dtd
ticket_delete.php	Delete tickets in the subscription. Managers and Unit Managers have permission to run this function. XML results returned using the ticket delete output DTD: https://qualysapi.qualys.com/ticket_delete_output.dtd
ticket_list_deleted.php	View a list of deleted tickets which the API user has permission to access. Managers have permission to run this function. XML results returned using the deleted ticket list output DTD: https://qualysapi.qualys.com/ticket_list_deleted_output.dtd
get_tickets.php	Get ticket information for selected tickets which the API user has permission to access. Methods for ticket selection are by ticket number or date/time since last update. XML results returned using the domain list DTD: https://qualysapi.qualys.com/remediation_tickets.dtd It's recommended to use the new ticket_list.php instead of get_tickets.php since the new function provides more functionality, including more ticket selection methods.

Ticket Selection Parameters

Functions for editing, viewing and deleting active tickets support several ticket selection parameters. Using these parameters you select which tickets in your account to take action on. Overdue and Invalid tickets are selected automatically, unless otherwise requested.

All ticket selection parameters are valid with these ticket functions: **`ticket_list.php`**, **`ticket_edit.php`** and **`ticket_delete.php`**. A small subset of these parameters is valid with the **`ticket_list_deleted.php`** function. None of these parameters is valid with **`get_tickets.php`** (see"Get Ticket Information" for information).

Parameters valid with all ticket functions (except **`get_tickets.php`**).

Parameter	Select these tickets
Ticket Numbers	
ticket_numbers={nnn,nnn-nnn,...}	Tickets with certain ticket numbers. Specify one or more ticket numbers and/or ranges. Use a dash (-) to separate the ticket range start and end. Multiple entries are comma separated.
since_ticket_number={value}	Tickets since a certain ticket number. Specify the lowest ticket number to be selected. Selected tickets will have numbers greater than or equal to the ticket number specified.
until_ticket_number={value}	Tickets until a certain ticket number. Specify the highest ticket number to be selected. Selected tickets will have numbers less than or equal to the ticket number specified.

Parameters valid with all ticket functions (except **`ticket_list_deleted.php`** and **`get_tickets.php`**).

Parameter	Select these tickets
Ticket Properties	
ticket_assignee={value}	Tickets with a certain assignee. Specify the user login of an active user account.
overdue={0|1}	Tickets that are overdue or not overdue. See "Overdue Tickets" below. When not specified, overdue and non-overdue tickets are selected. Specify 1 to select only overdue tickets. Specify 0 to select only tickets that are not overdue.

Parameter	Select these tickets
invalid={0 | 1}	Tickets that are invalid or valid. See "Invalid Tickets" below. When not specified, both valid and invalid tickets are selected. Specify 1 to select only invalid tickets. Specify 0 to select only valid tickets. You can select invalid tickets owned by other users, not yourself.
states={state}	Tickets with certain ticket state/status. See "Ticket State/Status" below. Specify one or more state/status codes. A valid value is OPEN (for state/status Open or Open/Reopened), RESOLVED (for state Resolved), CLOSED (for state/status Closed/Fixed), or IGNORED (for state/status Closed/Ignored). Multiple entries are comma separated. To select ignored vulnerabilities on hosts, specify: **`states=IGNORED`**
Ticket History	
modified_since_datetime={value}	Tickets modified since a certain date/time. Specify a date (required) and time (optional) since tickets were modified. Tickets modified on or after the date/time are selected. The start date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2006-01-01" or "2006-05-25T23:12:00Z".
unmodified_since_datetime={value}	Tickets not modified since a certain date/time. Specify a date (required) and time (optional) since tickets were not modified. Tickets not modified on or after the date/time are selected. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2006-01-01" or "2006-05-25T23:12:00Z".
Ticket Host Information	
ips={nnn,nnn-nnn,...}	Tickets on hosts with certain IP addresses. Specify one or more IP addresses and/or ranges. Multiple entries are comma separated.
asset_groups={ag1,ag2,...}	Tickets on hosts with IP addresses which are defined in certain asset groups. Specify the title of one or more asset groups. Multiple asset groups are comma separated. The title "All" may be specified to select all IP addresses in the user account.

Parameter	Select these tickets
dns_contains={value}	Tickets on hosts that have a NetBIOS host name which contains a certain text string. Specify a text string to be used. This string may include a maximum of 100 characters (ascii).
netbios_contains={value}	Tickets on hosts that have a NetBIOS host name which contains a certain text string. Specify a text string to be used. This string may include a maximum of 100 characters (ascii).
Ticket Vulnerability Information	
vuln_severities={1,2,3,4,5}	Tickets for vulnerabilities with certain severity levels. Specify one or more severity levels. Multiple levels are comma separated.
potential_vuln_severities={1,2,3,4,5}	Tickets for potential vulnerabilities with certain severity levels. Specify one or more severity levels. Multiple levels are comma separated.
qids={qid,qid,...}	Tickets for vulnerabilities with certain QIDs (Qualys IDs). Specify one or more QIDs. A maximum of 10 QIDs may be specified. Multiple QIDs are comma separated.
vuln_title_contains={value}	Tickets for vulnerabilities that have a title which contains a certain text string. The vulnerability title is defined in the KnowledgeBase. Specify a text string. This string may include a maximum of 100 characters (ascii).
vuln_details_contains={value}	Tickets for vulnerabilities that have vulnerability details which contain a certain text string. Vulnerability details provide descriptions for threat, impact, solution and results (scan test results, when available). Specify a text string. This string may include a maximum of 100 characters (ascii).
vendor_ref_contains={value}	Tickets for vulnerabilities that have a vendor reference which contains a certain text string. Specify a text string. This string may include a maximum of 100 characters (ascii).

Overdue Tickets

Each ticket has a due date for ticket resolution. The number of days allowed for ticket resolution is set as part of the policy rule configuration. Overdue tickets are those tickets for which the due date for resolution has passed.

Invalid Tickets

Tickets are invalid due to the changing status of the IP address or ticket owner. Regarding the IP address, a ticket is marked invalid when the ticket's IP address is removed from the ticket owner's account (applies to Unit Manager, Scanner, or Reader). Regarding the ticket owner, a ticket is marked invalid when the ticket owner's account is inactive, deleted, or the user's role was changed to "Contact".

Ticket State/Status

Several events trigger ticket updates as described earlier in "Ticket Update Events." Certain ticket updates result in changes to ticket state/status as indicated below.

Open refers to new and reopened tickets. Tickets are reopened in these cases: 1) when the service detected vulnerabilities for tickets with state/status Resolved or Closed/Fixed, and 2) when users or the service reopened Closed/Ignored tickets.

Resolved refers to tickets marked as resolved by users.

Closed/Fixed refers to tickets with vulnerabilities verified as fixed by the service.

Closed/Ignored refers to tickets ignored by users or the service (based on a user policy). Also, users can ignore vulnerabilities on hosts. If tickets exist for vulnerabilities set to ignore status, the service sets them to Closed/Ignored, and if tickets do not exist for these issues the service adds new tickets and changes them to Closed/Ignored. See "Set Vulnerabilities to Ignore on Hosts" for more information.

View Ticket List

ticket_list.php Function

The **ticket_list.php** function is used to view remediation ticket information from the user's Qualys account that can be integrated with third-party applications.

For performance reasons, a maximum of 1,000 tickets can be returned from a single **ticket_list.php** request. If this maximum is reached, the function returns a "Truncated after 1,000 records" message at the end of the XML output with the last ticket number included. Using an account with more than 1,000 tickets (or potentially more than 1,000 tickets), it is recommended that you write a script that makes multiple **ticket_list.php** requests until all tickets have been retrieved.

The function returns a remediation ticket list report. There are several input parameters available to filter the ticket list report to only include the tickets you want to see. For example, you can filter the list by ticket details, vulnerability details and host information. Note that only remediation tickets that the Qualys API user has permission to view are returned in the resulting report.

To view ticket information, use the following URL:

```
https://qualysapi.qualys.com/msp/ticket_list.php
```

The XML results returned by the **ticket_list.php** function identify tickets by ticket number with detailed ticket information, including general ticket information, host information, ticket statistics, ticket history, vulnerability detection information and vulnerability details, if requested.

Permissions

User permissions for the **ticket_list.php** function are described below.

User Role	Permissions
Manager	View tickets for all IP addresses in subscription.
Unit Manager	View tickets for IP addresses in user's business unit.
Scanner	View tickets for IP addresses in user's account.
Reader	View tickets for IP addresses in user's account.

Parameters

Several parameters for **ticket_list.php** allow you to select tickets to include in the ticket list. These parameters are described earlier in the section titled "Ticket Selection Parameters."All ticket selection parameters are optional. At least one ticket selection parameter is required. Multiple parameters are combined with a logical "and".

A display parameter for **ticket_list.php** allows you to specify whether vulnerability details will be included in the ticket list XML output. This parameter is:

```
show_vuln_details={0|1}
```

By default, vulnerability details are not included in the ticket list XML output. When set to **1**, vulnerability details are included. Vulnerability details provide descriptions for the threat posed by the vulnerability, the impact if exploited, the solution provided by Qualys as well as the scan test results (when available).

Examples

Using an account with more than 1,000 tickets (or potentially more than 1,000 tickets), it is recommended that you write a script that makes multiple **ticket_list.php** requests until all tickets are retrieved.

To view Open tickets owned by James Adrian (comp_ja), use the following URL:

```
https://qualysapi.qualys.com/msp/ticket_list.php?
ticket_assignee=comp_ja&states=OPEN
```

To view tickets from ticket #001800 to ticket #002800, use the following URL:

```
https://qualysapi.qualys.com/msp/ticket_list.php?
ticket_numbers=001800-002800
```

To view tickets on vulnerabilities and potential vulnerabilities with an assigned severity level of 5, use the following URL:

```
https://qualysapi.qualys.com/msp/ticket_list.php?
vuln_severities=5&potential_vuln_severities=5
```

To view tickets that have been marked as Closed/Fixed or Closed/Ignored since June 1, 2006, use the following URL:

```
https://qualysapi.qualys.com/msp/ticket_list.php?states=CLOSED,
IGNORED&modified_since_datetime=2006-06-01
```

If there are ignored vulnerabilities in your account, you can list all ignored vulnerabilities in the account using the following URL:

```
https://qualysapi.qualys.com/msp/ticket_list.php?asset_groups=
All&states=IGNORED
```

To view tickets related to SSH vulnerabilities, use the following URL:

```
https://qualysapi.qualys.com/msp/ticket_list.php?
vuln_title_contains=SSH&vuln_details_contains=SSH
```

To view Invalid tickets for hosts in the "Desktops" or "Servers" asset groups, use the following URL:

```
https://qualysapi.qualys.com/msp/ticket_list.php?asset_groups=
Desktops,Servers&invalid=1
```

To view Overdue tickets assigned to James Adrian (comp_ja) that have not been modified since September 30, 2005 at 16:30:00 (UTC/GMT) for vulnerabilities with a severity level of 3, 4 or 5 and to include vulnerability details in the results, use the following URL:

```
https://qualysapi.qualys.com/msp/ticket_list.php?
unmodified_since_datetime=2005-09-30T16:30:00Z
&vuln_severities=3,4,5&overdue=1&ticket_assignee=comp_ja
&show_vuln_details=1
```

XML Report

The DTD for the XML ticket list output returned by the **`ticket_list.php`** function can be found at the following URL:

```
https://qualysapi.qualys.com/ticket_list_output.dtd
```

Appendix E provides information about the XML report generated by the **`ticket_list.php`** function, including a recent DTD and XPath listing.

Edit Tickets

ticket_edit.php Function

The **ticket_edit.php** function is used to edit remediation tickets in a Qualys subscription. This function allows Managers and Unit Managers to edit multiple tickets at once "in bulk." Using this function Managers can make requests to change the ticket assignee, open and close tickets, flag Closed/Ignored tickets to be reopened automatically by the service, and add comments to tickets. Several input parameters are available for ticket selection. For example, these parameters support selecting tickets modified since a given date and/or since a given ticket number.

Upon success the **ticket_edit.php** function returns a report with ticket edit XML output with a listing of the edited tickets.

Editing tickets can be a time intensive task, especially when batch editing many tickets. To ensure best performance, a maximum of 20,000 tickets can be edited in one **ticket_edit.php** request. It's recommended best practice that you choose to schedule batch updates to occur when ticket processing will least impact user productivity. If the **ticket_edit.php** request identifies more than 20,000 tickets to be edited, then an error is returned.

Permissions

User permissions for the **ticket_edit.php** function are described below.

User Role	Permissions
Manager	Edit tickets for all IP addresses in subscription.
Unit Manager	Edit tickets for IP addresses in user's business unit.
Scanner	No permission to edit tickets.
Reader	No permission to edit tickets.

Parameters

The parameters for **ticket_edit.php** are described below. At least one ticket selection parameter is required, and one edit parameter is required.

Ticket Selection Parameters. Several parameters for **ticket_edit.php** allow you to select tickets to edit. These parameters are described earlier in the section titled "Ticket Selection Parameters." At least one ticket selection parameter is required. Multiple ticket selection parameters are combined with a logical "and".

Edit Parameters. The following parameters are used to specify the ticket data to be edited. At least one of the following edit parameters is required.

Parameter	Description
change_assignee={value}	(Optional) Used to change the ticket assignee, specified by user login, in all selected tickets. The assignee's account must have a user role other than Contact, and the hosts associated with the selected tickets must be in the user account.
change_state={value}	(Optional) Used to change the ticket state/status to the specified state/status in all selected tickets. A valid value is OPEN (for state/status Open and Open/Reopened), RESOLVED (for state Resolved), or IGNORED (for state/status Closed/Ignored). See "Ticket State/Status Transitions" below for information on valid changes.
add_comment={value}	(Optional) Used to add a comment in all selected tickets. The comment text may include a maximum of 2,000 characters (ascii).
reopen_ignored_days={value}	(Optional) Used to reopen Closed/Ignored tickets in a set number of days. Specify the due date in N days, where N is a number of days from today. A valid value is an integer from 1 to 730. When the due date is reached, the ticket state is changed from Closed/Ignored to Open, assuming the issue still exists, and the ticket is marked as overdue. If the issue was resolved at some point while the ticket was in the Closed/Ignored state, then the ticket state is changed from Closed/Ignored to Closed/Fixed.

Ticket State/Status Transitions

The Qualys remediation workflow feature is a closed loop ticketing system for remediation management and policy compliance. Users may edit tickets to make certain ticket state changes as shown below.

	To State/Status		
From State/Status	**Open**	**Resolved**	**Closed/Ignored**
Open	valid	valid	valid
Resolved	valid	valid	valid
Closed/Ignored	valid	invalid	valid
Closed/Fixed	valid	invalid	valid

See "Ticket State/Status" earlier in this chapter for more information.

Examples

To edit ticket #00123456 and add a comment, use this URL:

```
https://qualysapi.qualys.com/msp/ticket_edit.php?ticket_numbers
=00123456&add_comment=Host+patched,+ready+for+re-scan
```

To edit multiple tickets to change the ticket owner to Alice Cook (acme_ac) for tickets since ticket number #00215555 (tickets with numbers greater than or equal to #00215555) which are marked invalid, use this URL:

```
https://qualysapi.qualys.com/msp/ticket_edit.php?since_ticket_n
umber=00215555&invalid=1&change_assignee=acme_ac
```

To edit Open tickets on IP addresses in asset groups "New York" and "London" and change the ticket state to Ignored, use this URL:

```
https://qualysapi.qualys.com/msp/ticket_edit.php?states=OPEN&as
set_groups=New+York,London&change_state=IGNORED
```

To edit Open tickets unmodified since August 1, 2012 that are assigned to Tim Burke (acme_tb) and change the ticket assignee to Alice Cook (acme_ac), use this URL:

```
https://qualysapi.qualys.com/msp/ticket_edit.php?states=OPEN&un
modified_since=2012-08-01&ticket_assignee=acme_tb&change_assign
ee=acme_ac
```

To reopen all Closed/Ignored tickets on host 10.10.10.120 in 7 days, use this URL:

```
https://qualysapi.qualys.com/msp/ticket_edit.php?ips=10.10.10.1
20&reopen_ignored_days=7
```

XML Report

The DTD for the XML ticket edit output returned by the **`ticket_edit.php`** function can be found at the following URL:

```
https://qualysapi.qualys.com/ticket_edit_output.dtd
```

Appendix E provides information about the XML report generated by the **`ticket_edit.php`** function, including a recent DTD and XPath listing.

Delete Tickets

ticket_delete.php Function

The **ticket_delete.php** function is used to delete remediation tickets in a Qualys subscription. This function allows Managers and Unit Managers to delete multiple tickets at once "in bulk." Several input parameters are available for ticket selection. For example, these parameters support selecting tickets modified since a given date and/or since a given ticket number.

Upon success the **ticket_delete.php** function returns a report with ticket delete XML output with a listing of the deleted tickets.

Deleting tickets can be a time intensive task, especially when batch deleting many tickets. To ensure best performance, a maximum of 20,000 tickets can be deleted in one **ticket_delete.php** request. It's recommended best practice that you choose to schedule batch updates to occur when ticket processing will least impact user productivity. If the **ticket_delete.php** request identifies more than 20,000 tickets to be deleted, then an error is returned.

Permissions

User permissions for the **ticket_delete.php** function are described below.

User Role	Permissions
Manager	Delete tickets for all IP addresses in subscription.
Unit Manager	Delete tickets for IP addresses in same business unit.
Scanner	No permission to delete tickets.
Reader	No permission to delete tickets.

Parameters

Several parameters for **ticket_delete.php** allow you to select tickets to delete. These parameters are described earlier in the section titled "Ticket Selection Parameters." All ticket selection parameters are optional. At least one ticket selection parameter is required with each request. Multiple parameters are combined with a logical "and".

Examples

To delete ticket #002487, use this URL:

```
https://qualysapi.qualys.com/msp/ticket_delete.php?
ticket_numbers=2487
```

To delete tickets between ticket #001000 and ticket #002500, use the following URL:

```
https://qualysapi.qualys.com/msp/ticket_delete.php?
since_ticket_number=1000&until_ticket_number=2500
```

To delete Closed/Fixed tickets owned by James Adrian (comp_ja), use the following URL:

```
https://qualysapi.qualys.com/msp/ticket_delete.php?
states=CLOSED&ticket_assignee=comp_ja
```

To delete tickets on vulnerabilities with an assigned severity level of 1 and potential vulnerabilities with an assigned severity level of 1-3, use the following URL:

```
https://qualysapi.qualys.com/msp/ticket_delete.php?
vuln_severities=1&potential_vuln_severities=1,2,3
```

To delete Overdue tickets assigned to James Adrian (comp_ja) that have not been modified since July 04, 2006 at 12:00:00 (UTC/GMT), use the following URL:

```
https://qualysapi.qualys.com/msp/ticket_delete.php?
unmodified_since_datetime=2006-07-04T12:00:00Z
&overdue=1&ticket_assignee=comp_ja
```

XML Report

The DTD for the XML ticket delete output returned by the **`ticket_delete.php`** function can be found at the following URL:

```
https://qualysapi.qualys.com/ticket_delete_output.dtd
```

Appendix E provides information about the XML report generated by the **`ticket_delete.php`** function, including a recent DTD and XPath listing.

View Deleted Ticket List

ticket_list_deleted.php

The **ticket_list_deleted.php** function is used to view deleted tickets in the user's Qualys account. This function may be run by Managers. The functionality provided allows for real-time integration with third-party applications.

The XML results returned by the **ticket_list_deleted.php** function identifies deleted tickets by ticket number and deletion date/time.

For performance reasons, a maximum of 1,000 deleted tickets can be returned from a single **ticket_list_deleted.php** request. If this maximum is reached, the function returns a "Truncated after 1,000 records" message at the end of the XML report with the last ticket number included.

User permissions for the **ticket_list_deleted.php** function are described below.

User Role	Permissions
Manager	View deleted tickets for all IP addresses in subscription.
Unit Manager	No permission to view deleted tickets.
Scanner	No permission to view deleted tickets.
Reader	No permission to view deleted tickets.

Parameters

The parameters for **ticket_list_deleted.php** are described below. All parameters are optional. At least one parameter is required. Multiple parameters are combined with a logical "and".

Ticket Number Parameters. The following parameters are used to select deleted tickets by ticket number. These same parameters are available with other ticket functions.

Parameter	Description
ticket_numbers={nnn,nnn-nnn,...}	(Optional) Specifies certain ticket numbers. Specify one or more ticket numbers and/or ranges. Ticket range start and end is separated by a dash (-). Multiple entries are comma separated.

Parameter	Description
since_ticket_number={value}	(Optional) Specifies tickets since a certain ticket number. Specify the lowest ticket number to be selected. Selected tickets will have numbers greater than or equal to the ticket number specified.
until_ticket_number={value}	(Optional) Specifies tickets until a certain ticket number. Specify the highest ticket number to be selected. Selected tickets will have numbers less than or equal to the ticket number specified.

Deletion Date Parameters. The following parameters are used to select deleted tickets based on the date/time when tickets were deleted.

Parameter	Selects these tickets
deleted_since_datetime={value}	(Optional) Specifies tickets deleted since a certain date/time. Specify a date (required) and time (optional) to identify this timeframe. Tickets deleted on or after the date/time are selected. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT) like "2006-01-01" or "2006-05-25T23:12:00Z".
deleted_before_datetime={value}	(Optional) Specifies tickets deleted before a certain date/time. Specify a date (required) and time (optional) to identify this timeframe. Tickets deleted on or before the date/time are selected. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT) like "2006-01-01" or "2006-05-25T23:12:00Z".

Examples

To view tickets deleted from #000120 to #000200, use this URL:

```
https://qualysapi.qualys.com/msp/ticket_list_deleted.php?
ticket_numbers=120-200
```

To view tickets deleted since ticket number #000400, use this URL:

```
https://qualysapi.qualys.com/msp/ticket_list_deleted.php?
since_ticket_number=400
```

To view tickets deleted since June 1, 2006, use this URL:

```
https://qualysapi.qualys.com/msp/ticket_list_deleted.php?
deleted_since_datetime=2006-06-01
```

XML Report

The DTD for the XML deleted ticket list output returned by the **`ticket_list_deleted.php`** function can be found at the following URL:

```
https://qualysapi.qualys.com/ticket_list_deleted_output.dtd
```

Appendix E provides information about the XML report generated by the **`ticket_list_deleted.php`** function, including a recent DTD and XPath listing.

Get Ticket Information

get_tickets.php Function

Function Overview

The **get_tickets.php** function is used to view remediation ticket information from the user's Qualys account that can be integrated with third-party applications. The function returns a ticket information report. Only remediation tickets that the Qualys API user has permission to view are returned in the resulting ticket information report.

Qualys recommends that you run the **get_tickets.php** function two times a day, so that ticket updates due to the latest scan results and user productivity are made available in the ticket information reports.

User permissions for the **get_tickets.php** function are described below.

User Role	Permissions
Manager	View tickets for all IP addresses in subscription.
Unit Manager	View tickets for IP addresses in user's business unit.
Scanner	View tickets for IP addresses in user's account.
Reader	View tickets for IP addresses in user's account.

New ticket_list.php Function

Qualys has released a new function called **ticket_list.php**. It is recommended that you update to the new function which is described earlier in this chapter in the section "View Ticket List".

Parameters

The parameters for **get_tickets.php** are described below.

Parameter	Description
ticket_numbers={nnn,nnn,..}	(Optional) Specifies ticket numbers for which ticket information will be retrieved. Ticket numbers are integers, assigned by the service automatically. A maximum of 1,000 ticket numbers may be specified. Multiple ticket numbers are comma separated. This parameter or **since** must be specified.
since={value}	(Optional) Specifies the start date/time of the time window for retrieving tickets. Only tickets that have been updated within this time window will be retrieved. The end date/time of the time window for retrieving tickets is the date/time when **get_tickets.php** is run. The start date/time is specified in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT), like "2005-01-10T02:33:11Z". This parameter or **ticket_numbers** must be specified.
state={value}	(Optional) Specifies the current state of tickets to be retrieved. A valid value is OPEN, RESOLVED, or CLOSED. If unspecified, tickets with all states are retrieved.
vuln_details={0|1}	(Optional) Specifies whether vulnerability details will be retrieved. Vulnerability details include a description of the threat posed by the vulnerability, the impact if it is exploited, a verified solution, and in some cases test results returned by the scanning engine. By default, vulnerability details will not be retrieved. To retrieve vulnerability details, specify **vuln_details=1**.

Examples

To retrieve remediation tickets that have been updated since July 15, 2005 at 1:00:00 AM (UTC/GMT) and that have any state (Open, Resolved, or Closed), use the following URL:

```
https://qualysapi.qualys.com/msp/get_tickets.php?
  since=2005-07-15T01:00:00Z
```

To retrieve remediation tickets that have been updated since July 15, 2005 at 4:20:00 PM (UTC/GMT) and with the current state of Open, use the following URL:

```
https://qualysapi.qualys.com/msp/get_tickets.php?
  since=2005-07-15T16:20:00Z&state=OPEN
```

To retrieve remediation tickets 002737, 002738, and 002740 with vulnerability details, use the following URL:

```
https://qualysapi.qualys.com/msp/get_tickets.php?
  ticket_numbers=002737,002738,002740&vuln_details=1
```

XML Report

The DTD for the XML ticket information report returned by the **`get_tickets.php`** function can be found at the following URL:

```
https://qualysapi.qualys.com/remediation_tickets.dtd
```

Appendix E provides information about the XML report generated by the **`get_tickets.php`** function, including a recent DTD and XPath listing.

Host Functions

These Qualys API functions support host-level remediation management in the enterprise. These functions allow you to:

- View Host Information
- Set Vulnerabilities to Ignore on Hosts

The **get_host_info.php** function returns a host information report (get_host_info.dtd) based on the most recent host scan data available in the user account. Several parameters allow you to specify the amount of detail to include in the report to customize it as needed. The host scan data is part of a host's vulnerability history which is saved separately from saved scan results. For more information, see "Automatic Host Scan Data" in Chapter 5.

The **ignore_vuln.php** function allows you to ignore vulnerabilities on certain hosts. This functionality mirrors the ignored vulnerabilities feature available in the Qualys user interface. The **ignore_vuln.php** function returns a status message with a list of tickets that were modified.

An ignored vulnerability is defined to be a vulnerability on a certain host and port. Users may set vulnerabilities to ignore so that they are removed from automatic scan reports, host information reports, asset search portal results as well as other views in the Qualys user interface.

When your account has ignored vulnerabilities you can use **ignore_vuln.php** to restore (un-ignore) selected issues. Also since the service automatically creates tickets for ignored vulnerabilities, you have the option to un-ignore issues using the **ticket_delete.php** function. For more information, see "Delete Tickets" earlier in this chapter.

The sections that follow describe how to view host information using **get_host_info.php** and how to ignore vulnerabilities using **ignore_vuln.php**.

View Host Information

get_host_info.php Function

Function Overview

The **get_host_info.php** function is used to retrieve host information for a single host in the user's Qualys account. The function returns a host information report, which includes only the information that the user has permission to view.

Host information identifies a particular host and provides current security information about the host. The report returned by **get_host_info.php** identifies the host by its IP address, tracking method, and lists system information that was gathered during the most recent scan, such as DNS host name, NetBIOS host name (if applicable) and operating system. Additional information identifies the host's security risk rating, current vulnerabilities and tickets based on the host's most recent assessment data.

To obtain a host information report for IP address "64.41.134.60", use this URL:

```
https://qualysapi.qualys.com/msp/get_host_info.php?host_ip=64.41.134.60
```

Instead of an IP address, you may specify the DNS host name or the NetBIOS host name when the host name is available. See "Host Identification" for further information.

If you specify no parameters for a **get_host_info.php** request, the resulting report includes host parameters and standard host remediation data. Host parameters identify the host's IP address, DNS host name and NetBIOS host name when available, the operating system, and which host tracking method is enabled. Statistics on current vulnerabilities and tickets associated with the host are provided.

Several parameters allow you to request additional information to be included in the host information report. Multiple parameters may be specified for the desired report output.

Permissions

User permissions for the **get_host_info.php** function are described below.

User Role	Permissions
Manager	View host information for all IP addresses in subscription.
Unit Manager	View host information for IP addresses in user's business unit.
Scanner	View host information for IP addresses in user's account.
Reader	View host information for IP addresses in user's account.

Parameters

The parameters for **`get_host_info.php`** are described below.

Host Identification

Identify the host for which host information will be retrieved. You must specify one of these values: IP address, DNS or NetBIOS host name. The DNS or NetBIOS host name may be specified when the host name is available in your account. The service detects these host names when running scans, during host discovery.

The parameters for identifying the host are described below.

Parameter	Description
host_ip={value}	(Optional) Specifies the host's IP address.
host_dns={value}	(Optional) Specifies the host's DNS host name, as in "mycompany.com".
host_netbios={value}	(Optional) Specify the host's NetBIOS host name.

Vulnerability Levels

The parameters for specifying the vulnerability and severity levels to be included in the report are described below. By default all vulnerability and severity levels are included.

Parameter	Description
vuln_severity= {1,2,3,4,5 |all | none}	(Optional) Specifies whether confirmed vulnerabilities will be retrieved. By default, all confirmed vulnerabilities will be retrieved. Specify "none" to not retrieve any confirmed vulnerabilities. Specify one or more severity levels, 1 to 5 to retrieve certain severity levels. Multiple levels are comma separated.
potential_vuln_severity= {1,2,3,4,5 |all | none}	(Optional) Specifies whether potential vulnerabilities will be retrieved. By default, all potential vulnerabilities will be retrieved. Specify "none" to not retrieve any potential vulnerabilities. Specify one or more severity levels, 1 to 5, to retrieve certain severity levels. Multiple levels are comma separated.
ig_severity= {1,2,3,4,5 |all | none}	(Optional) Specifies whether information gathered detected on the host will be retrieved. By default, all information gathered will be retrieved. Specify "none" to not retrieve information gathered. Specify one or more severity levels, 1 to 3, to retrieve certain severity levels. Multiple levels are comma separated.

Additional Host Information

Identify whether additional information will be included in the host information report. By default, additional host information will not be included. These options are available:

General Information. User configurations associated with the host, including: the asset owner, asset groups, business units, authentication records that include the host, user accounts with permission to access the host, host attributes, and comments.

Vulnerability Information. Additional details on each current vulnerability, including the QID, severity level, title, category, detection history identifying how many times the host was scanned and the date and time of the last scan, and vulnerability details — the threat, impact, solution and scan test result descriptions. When CVSS scoring is enabled in the account, CVSS Base and Temporal scores are included.

Ticket Information. The ticket numbers associated with each current ticket sorted by ticket state (Open and Resolved) and by vulnerability severity level.

The parameters used to request additional host information are described below.

Parameter	Description
general_info={0|1}	(Optional) Specifies whether general information about the host will be retrieved. By default, general information will not be retrieved. To retrieve general information, specify **`general_info=1`**.
vuln_details={0|1}	(Optional) Specifies whether vulnerability details for the host will be retrieved. By default, vulnerability details will not be retrieved. To retrieve vulnerability details, specify **`vuln_details=1`**.
ticket_details={0|1}	(Optional) Specifies whether ticket details for the host will be retrieved. By default, ticket details will not be retrieved. To retrieve ticket details, specify **`ticket_details=1`**.

Examples

To retrieve host information for IP address “64.41.134.60”, use the following URL:

```
https://qualysapi.qualys.com/msp/get_host_info.php?host_ip=64.41.134.60
```

To retrieve host information for DNS host name“demo02.qualys.com”, use the following URL:

```
https://qualysapi.qualys.com/msp/get_host_info.php?host_dns=demo02.qualys.com
```

To retrieve host information for IP address “64.41.134.60” with general host information, vulnerability details, and ticket details, use the following URL:

```
https://qualysapi.qualys.com/msp/get_host_info.php?host_ip=64.4
1.134.60&general_info=1&vuln_details=1&ticket_details=1
```

XML Report

The DTD for the XML host information report returned by the **get_host_info.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/get_host_info.dtd
```

Appendix E provides information about the XML report generated by the **get_host_info.php** function, including a recent DTD and XPath listing.

Set Vulnerabilities to Ignore on Hosts

ignore_vuln.php Function

The **ignore_vuln.php** function is used to ignore or restore (un-ignore) vulnerabilities on certain hosts. The ignore status applies to a vulnerability/host pair. Vulnerabilities can be set to ignore on hosts so that they do not appear in automatic scan reports, host information reports, asset search reports as well as other views in the Qualys user interface.

Both Vulnerabilities and Potential Vulnerabilities may be set to the ignore status on hosts in the user's account. Information Gathered issues cannot be set to the ignore status. Note that the following QIDs cannot be set to ignore: 38175 (Unauthorized Service Detected), 82043 (Unauthorized Open Port Detected), 38228 (Required Service Not Detected) and 82051 (Required Port Not Detected).

When making an **ignore_vuln.php** request, you must specify QIDs (up to 10) and target hosts. Host selection parameters allow you to specify hosts by IP address, asset group, DNS host name or NetBIOS host name.

Target Hosts

A vulnerability can be set to ignore/restore only on hosts with scan results. If a host was previously scanned and then purged, the scan results are removed and no longer available. In this case an ignore vulnerability request will have no effect until a re-scan populates the host with fresh scan results.

The ignore/restore request applies to the target hosts at the time of the request. For example, if you specify an ignore action on asset groups, the request applies to the IP addresses in the asset groups at the time of the request. Subsequently, if an asset group is updated with new IP addresses, the new IPs are not set to the ignore status.

Ignored Status and Tickets

The ignore/restore actions have an effect on remediation tickets in the user account. When you set the ignore status for vulnerabilities on hosts, the service closes associated remediation tickets with the ticket state/status of Closed/Ignored. If no ticket exists, a new one will be created and closed automatically for tracking purposes as Closed/Ignored. When you restore vulnerabilities on hosts, the service automatically reopens the associated tickets and sets them to Open/Reopened.

The **ticket_list.php** function allows you to list tickets in the user account and this information could be useful for taking actions using **ignore_vuln.php**. For example, you could use **ticket_list.php** to find tickets on certain QIDs in the Closed/Ignored state and then use the information returned to make **ignore_vuln.php** requests to restore vulnerabilities on certain hosts.

Permissions

User permissions for the **ignore_vuln.php** function are described below.

User Role	Permissions
Manager	Ignore/Restore vulnerabilities and potential vulnerabilities on all hosts in subscription.
Unit Manager	Ignore/Restore vulnerabilities and potential vulnerabilities on hosts in user's business unit.
Scanner	Ignore/Restore vulnerabilities and potential vulnerabilities on hosts in user's account, when a certain remediation policy option is enabled. *
Reader	Ignore/Restore vulnerabilities and potential vulnerabilities on hosts in user's account, when a certain remediation policy option is enabled.*

* Scanners and Readers have permission to ignore/restore vulnerabilities when the option "Allow Scanners and Readers to mark tickets as Closed/Ignored" is enabled in the Qualys user interface. A Manager can edit this setting for the subscription. See the Qualys online help for information.

Parameters

The parameters for **ignore_vuln.php** are described below.

Request Parameters. The request parameters are below.

Parameter	Description
action=ignore | restore	A flag indicating an ignore or restore request. When unspecified, the action is set to "ignore". Specify "restore" to restore (un-ignore) vulnerabilities.
	Ignore request: Optional
	Restore request: Required
qids={qid,qid,...}	(Required) Specifies the QIDs (Qualys IDs) to ignore/restore. A maximum of 10 QIDs may be specified. Multiple QIDs are comma separated.

Parameter	Description
comments={value}	(Required) Specify comments for the action. The comments may include a maximum of 255 characters. Comments are stored with ignored vulnerabilities, and are visible to users in the Qualys user interface.
reopen_ignored_days={date}	(Optional) Set to reopen ignored vulnerabilities that are detected after a number of days (1-730). If the ignored vulnerability is reopened by the service, the corresponding ticket's state/status is changed from Closed/Ignored to Open/Reopened.

Host Selection Parameters. These host parameters are optional and mutually exclusive (only one may be specified per request). At least one parameter must be specified.

Parameter	Description
asset_groups={ag1,ag2,...}	(Optional) Selects hosts by asset group. The hosts included in the one or more asset groups provided are selected. A maximum of 5 asset group titles may be specified. The asset group title "All" as defined in the Qualys user interface may be specified. Multiple asset groups are comma separated.
	This parameter or another host selection parameter is required.
ips={nnn, nnn-nnn,...}	(Optional) Selects hosts by IP address. Enter one or more IP addresses and/or ranges. Multiple entries are comma separated. The parameter value may include a maximum of 512 characters (ascii).
	This parameter or another host selection parameter is required.
dns_contains={value}	(Optional) Selects hosts by DNS host name. Specify a text string contained in one or more DNS host names. The text string may include a maximum of 100 characters (ascii).
	This parameter or another host selection parameter is required.
netbios_contains={value}	(Optional) Selects hosts by NetBIOS host name. Specify a text string contained in one or more NetBIOS host names. The text string may include a maximum of 100 characters (ascii).
	This parameter or another host selection parameter is required.

Examples

To ignore QID 19070 "MS-SQL 8.0 UDP Slammer Worm Buffer Overflow Vulnerability" for the hosts in asset group "New York", use a URL like this:

```
https://qualysapi.qualys.com/msp/ignore_vuln.php?action=ignore&
qids=19070&asset_groups=New+York&comments=security+policy
```

To restore (un-ignore) QIDs 90305 and 100035 on IP address 10.10.10.33 and IP range 10.10.10.100-10.10.10.120, use a URL like this:

```
https://qualysapi.qualys.com/msp/ignore_vuln.php?action=restore
&qids=90305,100035&ips=10.10.10.33,10.10.10.100-10.10.10.120&co
mments=request+by+GStevenson
```

If there are ignored vulnerabilities in your account, you can list all ignored vulnerabilities in the account using the **ticket_list.php** function as shown in the following URL:

```
https://qualysapi.qualys.com/msp/ticket_list.php?asset_groups=
All&states=IGNORED
```

XML Report

The DTD for the XML ignored vulnerability output returned by the **ignore_vuln.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/ignore_vuln_output.dtd
```

Appendix E provides information about the XML report generated by the **ignore_vuln.php** function, including a recent DTD and XPath listing.

CHAPTER 7

User Management

Qualys supports adding users to a subscription, so that multiple users can participate in vulnerability management and policy compliance. For a new subscription the service provides one user account with full rights. Additional users may be granted full rights or limited rights depending on their user role and assigned assets. These assets include IP addresses for scans, domains for network discovery (maps) and scanner appliances for scanning the internal network.

This chapter describes how to add users to an existing subscription, update user account data, list users, and download action log reports. These topics are covered:

- About User Management
- User Management Functions
- Add/Edit Users
- User Registration Process
- Accept the Qualys EULA
- Activate/Deactivate Users
- View User List
- Download User Action Log Report
- User Password Change

About User Management

Users may be added to active Qualys subscriptions to distribute vulnerability management and policy compliance within the enterprise.

Qualys has a role-based model for granting privileges to users. These user roles are described below.

The most privileged users are Managers and Unit Managers. These users have the ability to manage assets and users. The main difference between Managers and Unit Managers is that Managers have management authority for the subscription (including any business units it may have), while Unit Managers have management authority on an assigned business unit only.

Scanners and Readers have limited rights on their assigned assets. Readers cannot run maps and scans, however they can view scan and map results, run reports, and view/edit remediation tickets.

Auditors may be added to a subscription when the compliance module is enabled in order to perform compliance management tasks. These users have limited rights on hosts that have been defined as compliance hosts for the subscription. While Auditors cannot run compliance scans, they can define policies and run reports based on compliance scan data.

All users have the option to receive summary email notifications at the completion of maps and scans for their permitted assets. The Contact user role grants users one privilege only to receive these summary notifications.

Please see the online help for further information about user roles and privileges.

User Management Functions

A summary of the user management functions that are available in the Qualys API are described below.

Function Name	Description
user.php	Add a user account to an existing subscription, edit an existing user account, activate a user account with an "Inactive" status, and deactivate a user account with an "Active" status. Managers and Unit Managers may use this function. XML results returned using the user output DTD: https://qualysapi.qualys.com/user_output.dtd
user_list.php	View a list of user accounts which the API user has permission to access. Managers and Unit Managers may view users using this function. XML results returned using the user list output DTD: https://qualysapi.qualys.com/user_list_output.dtd
action_log_report.php	Download user action log report for users which the API user has permission to view. Managers, Unit Managers, Scanners and Readers may view an action log report appropriate to their permission level. XML results returned using the action log report DTD: https://qualysapi.qualys.com/action_log_report.dtd
password_change.php	Change passwords for all or some users in the same subscription. Managers and Unit Managers may change passwords for multiple users at once using this function. Note the requesting user cannot change their own password. XML results returned using the password change output DTD: https://qualysapi.qualys.com/password_change_output.dtd

Add/Edit Users

user.php Function

Function Overview

The User API (**`/msp/user.php`**) is used to manage user accounts in an active Qualys subscription. With additional users, you can delegate responsibility across the organization. Using the **`user.php`** function, Managers and Unit Managers can add new user accounts and update existing accounts.

Express Lite: This API is available to Express Lite users. A total of 3 users can be added per subscription.

The API user can make a **`user.php`** request to add an account or edit an existing account. Upon success the function performs the requested update and returns an XML document indicating the status of the request as success or failure. For each new account (except when the user role is Contact) the service automatically generates login credentials, including a login ID and "strong" password.

To add a new user using **`user.php`**, there are several required parameters such as the user's name, general information, business unit and user role. Default parameters are set for email notifications and extended permissions (for Scanner or Unit Manager only). The account recipient can update these default settings using the Qualys user interface.

Using **`user.php`** you can add users to the "Unassigned" business unit or an existing, custom business unit. To add users to a custom business unit, follow these steps:

1. With a Manager account, log into the Qualys user interface and create the business unit. Note that business units may be created using the Qualys user interface only.
2. If a Unit Manager is not already assigned to the business unit, you must add one. With a Manager account, make a **`user.php`** request to add a Unit Manager who is automatically assigned as the business unit's point of contact (POC).
3. With a Manager or Unit Manager account, make a **`user.php`** request to add other users to the custom business unit. A Manager can add a user to any business unit, while a Unit Manager can add a user to their own business unit.

There are several default values when adding a new user. For more information, see "Default Parameters — New User".

When adding a new user (except Contact), the API user has the option to deliver login credentials directly to the user via email or through the application as follows.
By default the **`user.php`** function sends the new user an email notification with a secure link to their login credentials. When the user clicks the secure link to view the credentials, the service changes the account status automatically from "Pending Activation" to "Active". Instead of sending an email notification, the API user has the option to return

the new user's login credentials in the XML output document. To do this, make a **user.php** request with the **send_email=0** input parameter. As a result the service returns the user's login ID and password as XML value pairs in the XML output, and the account status is automatically set to "Active".

To complete account registration, a new user must log into the Qualys user interface with their assigned login information (platform URL and login credentials). When the user has been created using the **user.php** function the user can login using the Qualys user interface or using the acceptEULA.php API function. See "User Registration Process" and "Accept the Qualys EULA" or more information.

For an existing account, you can edit and clear account parameters as follows.

Edit Parameters. An existing user may be edited using **user.php** to update the user name, general information and user interface style. Additional parameters can be edited using the Qualys user interface. When editing parameters using **user.php**, existing parameter values are replaced with newly specified ones. For example, if you edit an existing Scanner with the assigned asset group "New York" and you wish to add the asset group "Hong Kong", then the edit request must include the parameter (for example, asset_groups=New+York,Hong+Kong).

Clear Parameters. When editing a user using **user.php**, an edit request can be used to clear (reset) parameters by assigning the empty string "". For example, if the user interface style is set to olive green and you want to reset the interface to the system default, which is standard blue, send an edit request with this parameter equal to empty string (ui_interface_style="").

User Permissions

User permissions for using the **user.php** function to create and edit user accounts are described below.

User Role	Permissions
Manager	Add user account to any business unit. Edit user data for any user account.
Unit Manager	Add user account to API user's same business unit. Edit user data for any user account in same business unit.
Scanner	No permission to add/edit user accounts.
Reader	No permission to add/edit user accounts.
Auditor	No permission to add/edit user accounts.

Parameters

The parameters for using the **user.php** function to create and edit user accounts are described below.

There are numerous parameters for **user.php**. Each parameter should appear at most once in a single API request. If the same parameter is specified multiple times, typically the last instance overrides the rest. Both GET and POST methods are supported. For more information, see "API Conventions" in Chapter 1.

Request Type

These parameters specify whether the request is to add or edit a user account.

Parameter	Description
action=add|edit	A flag indicating an add or edit request. Specify "add" to add a new user, or "edit" to edit an existing user.
	Add request: Required
	Edit request: Required
login={login}	Specifies the Qualys user login of the user account you wish to edit. This parameter is invalid for an add request.
	Add Request: Invalid
	Edit Request: Required

New User — Login Credentials

The **send_email** parameter may be specified when adding a new user account.

Parameter	Description
send_email={0|1}	(Optional) Specifies whether the new user will receive an email notification with a secure link to their login credentials. This parameter is invalid when the user role is Contact. 1 — (the default) specifies that an email notification will be sent to the new user. The user clicks a secure link in the email to view the login ID and password. 0 — specifies that an email notification will not be sent to the new user, and the XML report returned by the function will include the login ID and password for the user account as XML value pairs.
	Add request: Optional
	Edit request: Invalid

Permissions

When adding a user, you must specify the user role and business unit. For a Scanner, Reader or Contact, at least one asset group must be assigned to the user account.

Parameter	Description
user_role={role}	Specifies the user role. A valid value is: manager, unit_manager, scanner, reader, or contact. The first user added to a new custom business unit must be unit_manager.
	Add request: Required (Invalid for Express Lite user)
	Edit request: Invalid
business_unit={title}	Specifies the user's business unit. A valid value is "Unassigned", or the title of an existing custom business unit. Note a custom business unit may be added using the Qualys user interface.
	Add request: Required (Invalid for Express Lite user)
	Edit request: Invalid
asset_groups={grp1,grp2...}	Specifies the asset groups assigned to the user, when the user role is Scanner, Reader or Contact. Multiple asset groups are comma separated. This parameter is invalid when the user role is Manager or Unit Manager.
	Add request: Optional
	Edit request: Optional
ui_interface_style={style}	Specifies the user interface style. A valid value is: standard_blue, navy_blue, coral_red, olive_green, accessible_high_contrast. When adding a new user, the default is set to standard_blue.
	Add request: Optional
	Edit request: Optional

General Information

General information parameters are described below.

Parameter	Description
first_name={name}	Specifies the user's first name. The name may include a maximum of 50 characters.
	Add request: Required
	Edit Request: Optional

Parameter	Description
last_name={name}	Specifies the user's last name. The name may include a maximum of 50 characters.
	Add request: Required
	Edit request: Optional
title={title}	Specifies the user's job title. The title may include a maximum of 100 characters.
	Add request: Required
	Edit request: Optional
phone={value}	Specifies the user's phone number. This value may include a maximum of 40 characters.
	Add request: Required
	Edit request: Optional
fax={value}	The user's FAX number. This value may include a maximum of 40 characters.
	Add request: Optional
	Edit request: Optional
email={value}	Specifies the user's email address. The address must be a properly formatted address with a maximum of 100 characters.
	Add request: Required
	Edit request: Optional
address1={value}	Specifies the user's address line 1. This value may include a maximum of 80 characters.
	Add request: Required
	Edit request: Optional
address2={value}	Specifies the user's address line 2. This value may include a maximum of 80 characters.
	Add request: Optional
	Edit request: Optional
city={value}	Specifies the user's city. This value may include a maximum of 50 characters.
	Add request: Required
	Edit request: Optional

Parameter	Description
country={code}	Specifies the user's country code. See "Examples" to find an appropriate country code.
	Add request: Required
	Edit request: Optional
state={code}	Specifies the user's state code. A valid value depends on the country code specified for the **`country`** parameter. You must enter a state code using the **`state`** parameter when the country code is one of: "United States of America", "Australia", "Canada" or "India". See "State Codes" to find an appropriate state code. For other country codes, a state code does not need to be specified using the **`state`** parameter. If specified, enter the state code "none".
	Add request: Required for some country codes
	Edit request: Optional
zip_code={zipcode}	Specifies the user's zip code. This value may include a maximum of 20 characters. If not specified, this is set to the zip code in the API user's account.
	Add request: Optional
	Edit request: Optional
external_id={value}	Specify a custom external ID value. The external ID value can have a maximum of 256 characters, and it is case sensitive. The characters can be in uppercase, lowercase or mixed case. HTML or PHP tags cannot be included. Specify **`external_id=`** or **`external_id=""`** to delete an external ID value from an existing account.
	Add request: Optional
	Edit request: Optional

Set Timezone

Assign a timezone to a user using the optional parameter "time_zone_code".

Sample request Set the user profile to a specific timezone (i.e. pass timezone code).

```
https://qualysapi.qualys.com/msp/user.php?action=add&user_role=scanner&bu
siness_unit=Unassigned&asset_groups=New+York,Dallas&ui_interface_style=st
andard_blue&first_name=Chris&last_name=Woods&title=Security+Consultant&ph
```

```
one=2126667777&fax=2126667778&email=chris@mycompany.com&address1=500+Char
les_Avenue&address2=Suite+1260&city=New+York&country=United+States+of+Ame
rica&state=New+York&zip_code=10004&time_zone_code=US-NY
```

Sample request Set the user profile to the browser's timezone (i.e. pass empty/null).

```
https://qualysapi.qualys.com/msp/user.php?action=edit&login=acme_ab&time_
zone_code="
```

Looking for timezone codes? Use the time zone code list function to request the list (where qualysapi.qualys.com is your Qualys API server URL):

```
https://qualysapi.qualys.com/msp/time_zone_code_list.php
```

Default Parameters — New User

Several user parameters are set automatically when a new user is created. These are identified below. The parameter value *** is the value defined for the user account making the API request.

	Manager	Unit Manager	Scanner	Reader	Contact
General and User Role					
Zip code	***	***	***	***	***
Company	***	***	***	***	***
Interface Style	Standard Blue	Standard Blue	Standard Blue	Standard Blue	n/a
Language — KnowledgeBase	***	***	***	***	***
User Status	Pending activation	Pending activation	Pending activation	Pending activation	Active
Allow access to	GUI and API	GUI and API	GUI and API	GUI and API	n/a
Notification Options					
Latest Vulnerabilities	Weekly	Weekly	Weekly	Weekly	Weekly
Scan Summary	All	Scans on assigned groups	Scans on assigned groups	Scans on assigned groups	Scans on assigned groups
Map Summary	All	Maps on assigned groups	Maps on assigned groups	Maps on assigned groups	Maps on assigned groups
Daily Trouble Ticket Updates	NO	NO	NO	NO	n/a

	Manager	Unit Manager	Scanner	Reader	Contact
Extended Permissions					
Add assets	n/a	NO	n/a	n/a	n/a
Create option profiles	n/a	YES	YES	n/a	n/a
Purge host information/history	n/a	NO	NO	n/a	n/a
Create/edit remediation policy	n/a	NO	n/a	n/a	n/a
Create/edit authentication records	n/a	NO	n/a	n/a	n/a

Some of the default parameters values may be edited by the account users. For more information, see the Qualys online help.

Country Codes

Valid country codes:

Afghanistan | Albania | Algeria | Andorra | Angola | Anguilla | Antartica | Antigua and Barbuda | Argentina | Armenia | Aruba |Australia | Austria | Azerbaijan | Bahamas | Bahrain | Bangladesh | Barbados | Belarus | Belgium | Belize | Benin | Bermuda | Bhutan | Bolivia | Bosnia-Herzegovina | Botswana | Bouvet Island | Brazil | British Indian Ocean Territory | Brunei Darussalam | Bulgaria | Burkina Faso | Burundi | Cambodia | Cameroon | Canada | Cape Verde | Cayman Islands | Central African Republic | Chad | Chile | China | Christmas Island | Cocos (Keeling) Islands | Colombia | Comoros | Congo | Cook Islands | Costa Rica | Cote D'Ivoire | Croatia | Cuba | Cyprus | Czech Republic | Denmark | Djibouti | Dominica | Dominican Republic | East Timor | Ecuador | Egypt | El Salvador | Equatorial Guinea | Estonia | Ethiopia | Faeroe Islands | Falkland Islands (Malvinas) | Fiji | Finland | France | French Guiana | French Polynesia | French Southern Territories| Gabon | Gambia | Georgia | Germany | Ghana | Gibraltar | Greece | Greenland | Grenada | Guadeloupe | Guatemala | Guernsey, C.I. | Guinea | Guinea-Bissau | Guyana | Haiti | Heard and McDonald Islands | Honduras | Hong Kong | Hungary | Iceland | India | Indonesia | Iran (Islamic Republic of) | Iraq | Ireland | Isle of Man | Israel | Italy | Jamaica | Japan | Jersey, C.I. | Jordan | Kazakhstan | Kenya | Kiribati | Korea | Kuwait | Kyrgyzstan | Lao Peoples Democratic Republi | Latvia | Lebanon | Lesotho | Liberia | Libyan Arab Jamahiriya | Liechtenstein | Lithuania | Luxembourg | Macau | Macedonia | Madagascar| Malawi | Malaysia | Maldives | Mali | Malta | Marshall Islands | Martinique | Mauritania | Mauritius | Mexico | Micronesia, Fed. States of | Moldova, Republic of | Monaco | Mongolia | Montserrat | Morocco | Mozambique | Myanmar | Namibia | Nauru | Nepal | Netherland Antilles | Netherlands | Neutral Zone (Saudi/Iraq) | New Caledonia | New Zealand | Nicaragua | Niger | Nigeria | Niue | Norfolk Island | Northern Mariana Islands | Norway | Oman | Pakistan | Palau | Panama Canal Zone | Panama | Papua New Guinea | Paraguay | Peru | Philippines | Pitcairn | Poland | Portugal | Puerto Rico | Qatar | Reunion | Romania | Russia | Rwanda | Saint Kitts and Nevis | Saint Lucia | Samoa | San Marino | Sao Tome and Principe | Saudi Arabia | Senegal | Seychelles | Sierra Leone | Singapore | Slovak Republic | Slovenia | Solomon Islands | Somalia | South Africa | Spain | Sri Lanka | St. Helena | St. Pierre and Miquelon | St. Vincent and the Grenadines | Sudan | Suriname | Svalbard and Jan Mayen Islands | Swaziland | Sweden | Switzerland | Syrian Arab Republic | Taiwan | Tajikistan | Tanzania, United Republic of | Thailand | Togo | Tokelau | Tonga | Trinidad and Tobago | Tunisia | Turkey | Turkmenistan | Turks and Caicos Islands | Tuvalu | U.S.Minor Outlying Islands |

Uganda | Ukraine | United Arab Emirates | United Kingdom | United States of America | Uruguay | Uzbekistan | Vanuatu | Vatican City State | Venezuela | Vietnam | Virgin Islands (British) | Wallis and Futuna Islands | Western Sahara | Yemen | Yugoslavia | Zaire | Zambia | Zimbabwe

State Codes

State Codes for United States

Value state codes when country is "United States of America":

Alabama | Alaska | Arizona | Arkansas | Armed Forces Asia | Armed Forces Europe | Armed Forces Pacific | California | Colorado | Connecticut | Delaware | District of Columbia |Florida | Georgia | Hawaii | Idaho | Illinois | Indiana | Iowa | Kansas | Kentucky | Louisiana | Maine | Maryland | Massachusetts | Michigan | Minnesota | Mississippi | Missouri | Montana | Nebraska | Nevada | New Hampshire | New Jersey| New Mexico | New York | North Carolina | North Dakota | Ohio | Oklahoma | Oregon | Pennsylvania | Rhode Island |South Carolina | South Dakota | Tennessee | Texas | Utah | Vermont | Virginia | Washington | West Virginia | Wisconsin | Wyoming

State Codes for Australia

Valid state codes when country is "Australia":

No State | New South Wales | Northern Territory | Queensland | Tasmania | Victoria | Western Australia

State Codes for Canada

Valid state codes when country is "Canada":

No State | Alberta | British Columbia | Manitoba | New Brunswick | Newfoundland | Northwest Territories | Nova Scotia | Nunavut | Ontario | Prince Edward Island | Quebec | Saskatchewan | Yukon

State Codes for India

Valid state codes when country is "India":

No State | Andhra Pradesh | Andaman and Nicobar Islands | Arunachal Pradesh | Assam | Bihar | Chandigarh | Chattisgarh | Dadra and Nagar Haveli | Daman and Diu | Delhi | Goa | Gujarat | Haryana | Himachal Pradesh | Jammu and Kashmir | Jharkhand | Karnataka | Kerala | Lakshadadweep | Madhya Pradesh | Maharashtra | Manipur | Meghalaya | Mizoram | Nagaland | Orissa | Pondicherry | Punjab |Rajasthan |Sikkim | Tamil Nadu | Tripura | Uttar Pradesh | Uttaranchal | West Bengal

Examples

Use this URL to add a new user, Chris Woods, to the Unassigned business unit with the Scanner user role, assign the user two asset groups, and automatically send the user an email notification with a secure link to his login credentials:

```
https://qualysapi.qualys.com/msp/user.php?action=add&user_role=
scanner&business_unit=Unassigned&asset_groups=New+York,Dallas&u
i_interface_style=standard_blue&first_name=Chris&last_name=Wood
s&title=Security+Consultant&phone=2126667777&fax=2126667778&ema
il=chris@mycompany.com&address1=500+Charles_Avenue&address2=Sui
te+1260&city=New+York&country=United+States+of+America&state=Ne
w+York&zip_code=10004
```

Use this URL to edit the Chris Woods account to add the asset group "Atlanta":

```
https://qualysapi.qualys.com/msp/user.php?action=edit&login=myc
orp_cw&asset_groups=New+York,Dallas,Atlanta
```

Use this URL to edit the Chris Woods account and change the user interface style:

```
https://qualysapi.qualys.com/msp/user.php?action=edit&login=myc
orp_cw&ui_interface_style=olive_green
```

To add the external ID "Qualys123" to the existing user account "qualys_ab5" when that account does not already have an external ID:

```
https://qualysapi.qualys.com/msp/user.php?action=edit&
login=qualys_ab5&external_id=Qualys123
```

To add the external ID "Qualy123" to the existing user account "qualys_ab" when that account already has an external ID:

```
https://qualysapi.qualys.com/msp/user.php?action=edit&
login=qualys_ab5&external_id=Qualys123
```

To delete the external ID currently defined for the user account "qualys_ab5":

```
https://qualysapi.qualys.com/msp/user.php?action=edit&
login=qualys_ab5&external_id=
```

XML Report

The DTD for the XML user output returned by the **user.php** function can be found at the following URL (where "qualysapi.qualys.com" is the Qualys API server where your account is located):

```
https://qualysapi.qualys.com/user_output.dtd
```

Appendix F provides information about the XML report generated by the **user.php** function, including a recent DTD and XPath listing.

User Registration Process

When a new user account is created, the service by default sends the user an email titled "Registration - Start Now". This email includes a secure link to the user's login information — platform URL and login credentials. Instead of sending an email notification, the API user has the option to return login credentials using **`user.php`** function with the **`send_email=0`** input parameter.

The user must complete the first login to the service in order to complete the account registration and accept the Qualys EULA (End User License Agreement). When the first login is completed, the service sends the user an email titled "Registration - Complete".

A new user has the option to complete the first login by simply logging into the Qualys user interface, as long as the user is granted the GUI access method. (Note a new user created using the **`user.php`** function is automatically granted the GUI and API access methods.) Using the Qualys user interface, the user is directed to the First Login form to complete the registration and accept the Qualys EULA.

The **`acceptEULA.php`** API function is provided as a programmatic method for completing the registration and accepting the Qualys EULA. To use complete the first login using the **`acceptEULA.php`** function, the user must submit an API request using their platform URL and login credentials.

Important: If a new user account is created using the Qualys user interface and the account is granted the API access method only (without the GUI access method), the user must complete the first login using the **`acceptEULA.php`** API function. If the **`acceptEULA.php`** API request is not made or it is not successful, the new account will not be activated and any API requests submitted using the new account will fail.

Accept the Qualys EULA

acceptEULA.php Function

Function Overview

The **acceptEULA.php** function allows Qualys users to complete the registration process and accept the Qualys End User License Agreement (EULA) on behalf of their customers. This function provides programmatic acceptance of the Qualys EULA.

A new user can complete the registration process and accept the Qualys EULA through the Qualys user interface as long as their account is granted the GUI access method. (Note a new user created using the **user.php** function is automatically granted the GUI and API access methods.) Optionally, a new user can complete the registration and accept the Qualys EULA using the **acceptEULA.php** function. See "User Registration Process" for information.

A Web application that allows Qualys EULA acceptance can be setup as follows. Inside the third party web application, a developer can setup a Web form that displays the Qualys EULA and has an "I Accept" button. A new Qualys user opens the Web form in a browser, reads the EULA description and clicks "I Accept" in the Web form. The third party's program submits an HTTP request to the Qualys API server using the **acceptEULA.php**. Along with the **acceptEULA.php** URL, the application must send Qualys user account credentials (login and password) as part of the HTTP request.

User Permissions

User permissions for using the **acceptEULA.php** function to complete the user registration process and accept the Qualys EULA are described below.

User Role	Permissions
Manager	Complete user registration and accept EULA.
Unit Manager	Complete user registration and accept EULA.
Scanner	Complete user registration and accept EULA.
Reader	Complete user registration and accept EULA.
Auditor	Complete user registration and accept EULA.

Example

To accept the Qualys EULA on behalf of a user, use the following URL:

```
https://qualysapi.qualys.com/msp/acceptEULA.php
```

XML Success Message

The **acceptEULA.php** function returns an XML success message like this:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE GENERIC_RETURN SYSTEM
"https://qualysapi.qualys.com/generic_return.dtd">
<GENERIC_RETURN>
<API name="acceptEULA.php" username="rob" at="2002-05-
10T13:44:23" />
<RETURN status="SUCCESS">
      TNC accepted within MSP
 </RETURN>
</GENERIC_RETURN>
```

The DTD for the message returned by the **acceptEULA.php** function can be found at the following URL:

```
https://qualysapi.qualys.com/generic-return.dtd
```

Activate/Deactivate Users

user.php Function

Function Overview

The User API (/msp/**`user.php`**) is used to manage user accounts in an active Qualys subscription. With additional users, you can delegate responsibility across the organization. Using the **`user.php`** function, Managers and Unit Managers can add new user accounts and update existing accounts.

Express Lite: This API is available to Express Lite users.

The API user can make a **`user.php`** request to activate and deactivate user accounts. These actions correspond to the activate/deactivate options in the Qualys UI. Note new accounts are activated by default after the user completes the account activation process (registration) by logging into the service for the first time. Upon success the function performs the requested update and returns an XML document indicating the status of the request as success or failure.

User Permissions

User permissions for using the **`user.php`** function to activate and deactivate user accounts are described below.

User Role	Permissions
Manager	Activate any user account that has an "Inactive" status. Deactivate any user account that has an "Active" status.
Unit Manager	Activate a user account which is in the user's business unit and which has an "Inactive" status. Deactivate a user account which is in the user's business unit and which has an "Active" status.
Scanner	No permission to activate/deactivate user accounts.
Reader	No permission to activate/deactivate user accounts.
Auditor	No permission to activate/deactivate user accounts.

Parameters

The parameters for using the **user.php** function to activate and deactivate user accounts are described below.

Parameter	Description
action=activate | deactivate	(Required) A flag indicating the desired action. Specify "activate" to activate a user account that has an "Inactive" status, or specify "deactivate" to deactivate a user account that has an "Active" status. When an account is deactivated, the user's account settings will not be deleted. A user account cannot be activated or deactivated if the account status is "Pending Activation".
login={login}	(Required) Specifies the Qualys user login for the user account you wish to activate or deactivate.

Examples

Sample **user.php** API requests that demonstrate how to activate/deactivate a user account are provided below. Note the syntax used assumes "qualysapi.qualys.com" is the name of the Qualys API server where the user's account is located.

To deactivate the user account "qualys_ab3" (and this account has an "Active status):

```
https://qualysapi.qualys.com/msp/user.php?action=deactivate&
login=qualys_ab3
```

To activate the user account "qualys_ab3" (and this account has an "Inactive" status):

```
https://qualysapi.qualys.com/msp/user.php?action=activate&
login=qualys_ab3
```

XML Report

The DTD for the XML user output returned by the **user.php** function can be found at the following URL (where "qualysapi.qualys.com" is the Qualys API server where your account is located):

```
https://qualysapi.qualys.com/user_output.dtd
```

Appendix F provides information about the XML report generated by the **user.php** function, including a recent DTD and XPath listing.

View User List

user_list.php Function

The User List API (**/msp/user_list.php**) is used to view the users in the subscription. To view the users in the subscription, use the following URL:

```
https://qualysapi.qualys.com/msp/user_list.php
```

Express Lite: This API is available to Express Lite users.

The XML results returned by the **user_list.php** function provide details about each user, such as the user's login ID, general information, assigned asset groups, user interface style, and extended permissions.

When the API request is made by a Manager or Unit Manager, the last login date for each user is provided in the XML results. This is the most recent date and time the user logged into the service. For a Manager, the last login date appears for all users in the subscription. For a Unit Manager, the last login date appears for all users in the Unit Manager's same business unit.

User permissions for the **user_list.php** function are described below.

User Role	Permissions
Manager	View all user accounts in the subscription with full details.
Unit Manager	See "Unit Manager Permissions" below.
Scanner	No permission to view user accounts.
Reader	No permission to view user accounts.
Auditor	No permission to view user accounts.

Unit Manager Permissions

Unit Managers can view full user account details for users in their business unit. Unit Managers may also be able to view partial user account details for users outside of their business unit. This is determined by a subscription level permission set by Managers in the user interface.

If "Restrict view of user information for users outside of business unit" is not selected (the default), then Unit Managers have an unrestricted view and can see partial details about users who are not in their assigned business unit.

If "Restrict view of user information for users outside of business unit" is selected, then Unit Managers have a restricted view and cannot see any details for users who are not in their assigned business unit. For example, Unit Managers in Business Unit A would not be able to view general information or asset group assignments for users in Business Unit B.

The following table describes the amount of detail visible to Unit Managers for different types of users based on whether the Unit Manager has a restricted or unrestricted view.

	Amount of Detail Visible	
User Type Being Viewed	**Unrestricted View**	**Restricted View**
Unit Manager, Scanner or Reader in the business unit	Full	Full
Scanner or Reader not in the business unit	Partial	None
Unit Manager not in the business unit	Partial	None
Manager	Partial	None

Full user account details include: user login, general information, assigned asset groups, user role, business unit, the Unit Manager Point of Contact (POC), the Manager POC, extended permissions, email notifications and user interface style.

With a Partial view, the following details are not visible: user login, extended permissions, email notifications and user interface style.

Parameters

The optional parameters available for the **user_list.php** function are described below. These parameters are mutually exclusive.

Parameter	Description
external_id_contains={string}	(Optional) Show only user accounts with an external ID value that contains a certain string. The string you specify can have a maximum of 256 characters. The characters can be in uppercase, lowercase or mixed case (the service performs case sensitive matching). HTML or PHP tags cannot be included. Only one of these parameters may be specified for a single API request: **external_id_contains** or **external_id_assigned**.
external_id_assigned={0|1}	(Optional) Specify 1 to show only user accounts which have an external ID value assigned. Specify 0 to show only user accounts which do not have an external ID value assigned. Only one of these parameters may be specified for a single API request: **external_id_contains** or **external_id_assigned**.

XML Report

The DTD for the XML user list output returned by the **user_list.php** function can be found at the following URL (where "qualysapi.qualys.com" is the Qualys API server where your account is located):

```
https://qualysapi.qualys.com/user_list_output.dtd
```

Appendix F provides information about the XML report generated by the **user_list.php** function, including a recent DTD and XPath listing.

Download User Action Log Report

action_log_report.php Function

The Action Log API (**/msp/action_log_report.php**) is used to download a report of user actions recorded in the user action log for the subscription. You can download actions performed by all users over any 3 month range and filter the list to only include actions performed by a particular user.

To download the user action log report, use a URL like this:

```
https://qualysapi.qualys.com/msp/action_log_report.php?
date_from=2006-06-01
```

Express Lite: This API is available to Express Lite users.

The XML results returned by the **action_log_report.php** function provide details about recorded user actions, such as the date/time of the action, the user who performed the action, the user's IP address from which the action was initiated and other details.

User permissions for the **action_log_report.php** function are described below.

User Role	Permissions
Manager	Download an action log report with actions performed by all users in the subscription.
Unit Manager	Download an action log report with actions performed by all users within the user's business unit.
Scanner	Download an action log report with the user's own actions.
Reader	Download an action log report with the user's own actions.
Auditor	No permission to download action log reports.

Types of actions recorded in the action log include:

- Log in and Log out
- Launch maps and scans (on demand and scheduled)
- Completion of maps and scans
- Pause and resume scans
- Create, edit, and delete various account configurations, such as asset groups, option profiles, report templates and scheduled tasks
- Change password
- Change security settings (Manager only)

Parameters

The parameters for **action_log_report.php** are described below.

Parameter	Description
date_from={value}	(Required) Specifies the start date/time of the time window for downloading action log entries. The start time is optional. The start date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT) like "2006-01-01" or "2006-05-25T23:12:00Z". If a start time is not specified, then the time is automatically set to the start of the day: T00:00:00Z
date_to={value}	(Optional) Specifies the end date/time of the time window for downloading action log entries. The end date must be later than the start date and not exceed 3 months. The end date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT) like "2006-01-01" or "2006-05-25T23:12:00Z". If an end date is not specified, the end date is automatically set to the current date and time when **action_log_report.php** is run. If an end date is supplied without an end time, then the time is automatically set to the end of the day: T23:59:59Z.
user_login={value}	(Optional) Specifies a Qualys user login ID. This parameter may be specified by a Manager or Unit Manager to filter results to only download actions performed by the specified user.

Examples

To download all user actions since May 1, 2006, use the following URL:

```
https://qualysapi.qualys.com/msp/action_log_report.php?
date_from=2006-05-01
```

To download user actions between May 1, 2006 and June 1, 2006, use the following URL:

```
https://qualysapi.qualys.com/msp/action_log_report.php?
date_from=2006-05-01&date_to=2006-06-01
```

To download all user actions performed by user ID "john_doe" since July 15, 2006 at 16:30:00 (UTC/GMT), use the following URL:

```
https://qualysapi.qualys.com/msp/action_log_report.php?
date_from=2006-07-15T16:30:00Z&user_login=john_doe
```

XML Report

The DTD for the XML action log report returned by the **action_log_report.php** function can be found at the following URL (where "qualysapi.qualys.com" is the Qualys API server where your account is located):

```
https://qualysapi.qualys.com/action_log_report.dtd
```

Appendix F provides information about the XML report generated by the **action_log_report.php** function, including a recent DTD and XPath listing.

Action Log Details

Each action log entry in the action log report includes the following details:

- Date and time of the action
- Module affected by the action
- Action performed (e.g. create, update, delete)
- Specific details of the action (e.g. changes made to a scheduled task)
- Qualys user login ID for the user who performed the action
- Name of the user who performed the action
- User role assigned to the user who performed the action
- IP address of the user system from which the action was initiated

Refer to "Actions and Modules" in the Qualys online help for a current listing.

User Password Change

password_change.php Function

The Password Channge API (**/msp/password_change.php**) is used to change passwords for all or some users in the same subscription. Many Qualys customers have an internal security policy requirement to change passwords for users at a particular time interval. This function allows Managers and Unit Managers to change passwords for multiple users at once as a "batch" process. New passwords are automatically generated by the service.

Express Lite: This API is available to Express Lite users.

Using the **password_change.php** function you can change passwords for user accounts with a status of "active", "inactive" or "pending activation". It's not possible to change passwords for deleted accounts. Since Contact users do not have login access to Qualys, it's not possible to change passwords for Contacts.

The **password_change.php** function returns a password change XML report indicating the user accounts affected and whether password changes were made for each account. A success message is included when passwords were changed on all target accounts. A warning message is included if passwords for any of the target accounts could not be changed. Upon error, an error message is included.

By default the password changes made by the **password_change.php** function causes the service to automatically send each affected user an email which notifies them of the password change. If you do not wish users to receive this email notification, you have the option to return the user login ID and password for affected users as XML value pairs in the password change report. To do this, make a **password_change.php** request and specify the **email=0** parameter. If you make such a request on an account with the status "pending activation", the function automatically assigns the "active" status since the login credentials are available in the XML report.

Permissions

User permissions for the **password_change.php** function are described below. Note this function cannot be used to change the password of the requesting user (Manager or Unit Manager).

User Role	Permissions
Manager	Change passwords for all users in subscription, except the user making the request.
Unit Manager	Change passwords for all users in same business unit, except the user making the request.
Scanner	No permission to change passwords.

User Role	Permissions
Reader	No permission to change user passwords.
Auditor	No permission to change user passwords.

Parameters

The parameters for **`password_change.php`** are described below.

Parameter	Description
user_logins={value}	(Required) Specifies one or more Qualys user login IDs of target user accounts. Multiple user login IDs are comma separated. Specify **`user_logins=all`** to change the password for all users in the user's account, except the requesting user. See the "Permissions" section for more information.
email={0|1}	(Optional) Specifies whether users will receive an email notification alerting them to the password change. 1 — (the default) specifies that an email notification will be sent to affected users. Each user clicks a secure link in the email to view the new password. 0 — specifies that email notifications will not be sent to affected users, and the XML report returned by the function will include the login ID and password for each user account as XML value pairs.

Examples

To make a password change request for two accounts and send affected users an email notification including a secure link to their new password, use this URL:

```
https://qualysapi.qualys.com/msp/password_change.php?
user_logins=acme_jr,acme_dd
```

To make a password change request for all users in the API user's account (except the API user) and return the login ID and password for each affected user in the password change XML report, use this URL:

```
https://qualysapi.qualys.com/msp/password_change.php?
user_logins=all&email=0
```

XML Report

The DTD for the XML password change output returned by the **password_change.php** function can be found at the following URL (where "qualysapi.qualys.com" is the Qualys API server where your account is located):

```
https://qualysapi.qualys.com/password_change_output.dtd
```

Appendix F provides information about the XML report generated by the **password_change.php** function, including a recent DTD and XPath listing.

APPENDIX A

Vulnerability Scan Reports

This appendix provides details about the XML output returned by vulnerability scan functions and the KnowledgeBase download function:

- Scan Results
- Scan Report List
- Running Scans and Maps List
- Scan Target History Output
- KnowledgeBase Download Output

Scan Results

The vulnerability scan results report is an XML report returned from the functions: **scan.php** and **scan_report.php**. The scan report includes summary and host-based results.

A selective vulnerability scan may be performed when the option profile is configured to scan user-selected vulnerabilities. If certain checks are not included, then certain vulnerability assessment data will not be available in your scan results and related vulnerability history in other scan reports and views in the user interface. For more information, see "Scan Results and Host Scan Data" in Chapter 5.

The report summary in the header section provides summary information about the scan, including the user who requested the scan, the time when the scan was initiated, the target hosts, and how long the scan took to complete. Host-based results include detailed information on vulnerabilities detected for each scanned host.

DTD for Vulnerability Scan Results

A recent **scan-1.dtd** is shown below.

```
<!-- QUALYS SCAN DTD -->

<!ELEMENT SCAN ((HEADER | ERROR | IP)+)>
<!ATTLIST SCAN
    value CDATA #REQUIRED
>
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR
    number CDATA #IMPLIED
>
<!-- INFORMATION ABOUT THE SCAN -->
<!ELEMENT HEADER (KEY+, ASSET_GROUPS?, ASSET_TAG_LIST?, OPTION_PROFILE?)>
<!ELEMENT KEY (#PCDATA)>
<!ATTLIST KEY
    value CDATA #IMPLIED
>

<!-- NAME of the asset group with the TYPE attribute with possible values
of (DEFAULT | EXTERNAL | ISCANNER) -->
<!ELEMENT ASSET_GROUP (ASSET_GROUP_TITLE)>
<!ELEMENT ASSET_GROUPS (ASSET_GROUP+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>
<!ELEMENT OPTION_PROFILE (OPTION_PROFILE_TITLE)>
<!ELEMENT OPTION_PROFILE_TITLE (#PCDATA)>
<!ATTLIST OPTION_PROFILE_TITLE
    option_profile_default CDATA #IMPLIED
>
```

```
<!-- TAGSET -->
<!ELEMENT ASSET_TAG_LIST (INCLUDED_TAGS?, EXCLUDED_TAGS?)>
<!ELEMENT INCLUDED_TAGS (ASSET_TAG+)>
<!ELEMENT EXCLUDED_TAGS (ASSET_TAG+)>
<!ELEMENT ASSET_TAG (#PCDATA)>
<!ATTLIST INCLUDED_TAGS scope (any|all) #REQUIRED>
<!ATTLIST EXCLUDED_TAGS scope (any|all) #REQUIRED>

<!-- IP -->
<!ELEMENT IP (OS?, OS_CPE?, NETBIOS_HOSTNAME?, INFOS?, SERVICES?, VULNS?,
              PRACTICES?)>
<!ATTLIST IP
    value CDATA #REQUIRED
    name CDATA #IMPLIED
    status CDATA #IMPLIED
>
<!ELEMENT OS (#PCDATA)>
<!ELEMENT OS_CPE (#PCDATA)>
<!ELEMENT NETBIOS_HOSTNAME (#PCDATA)>
<!-- CATEGORIES OF INFO, SERVICE, VULN or PRACTICE -->
<!ELEMENT CAT (INFO+ | SERVICE+ | VULN+ | PRACTICE+)>
<!ATTLIST CAT
    value CDATA #REQUIRED
    fqdn CDATA #IMPLIED
    port CDATA #IMPLIED
    protocol CDATA #IMPLIED
    misc CDATA #IMPLIED
>
<!-- IP INFORMATIONS -->
<!ELEMENT INFOS (CAT)+>
<!ELEMENT INFO (TITLE, LAST_UPDATE?, PCI_FLAG, INSTANCE?,
                VENDOR_REFERENCE_LIST?, CVE_ID_LIST?, BUGTRAQ_ID_LIST?,
                DIAGNOSIS?, DIAGNOSIS_COMMENT?, CONSEQUENCE?,
                CONSEQUENCE_COMMENT?, SOLUTION?, SOLUTION_COMMENT?,
                COMPLIANCE?, CORRELATION?, RESULT?)>
<!ATTLIST INFO
    severity CDATA #IMPLIED
    standard-severity CDATA #IMPLIED
    number CDATA #IMPLIED
>
<!-- MAP OF SERVICES -->
<!ELEMENT SERVICES (CAT)+>
<!ELEMENT SERVICE (TITLE, LAST_UPDATE?, PCI_FLAG, INSTANCE?,
                   VENDOR_REFERENCE_LIST?, CVE_ID_LIST?, BUGTRAQ_ID_LIST?,
                    DIAGNOSIS?, DIAGNOSIS_COMMENT?, CONSEQUENCE?,
                    CONSEQUENCE_COMMENT?, SOLUTION?, SOLUTION_COMMENT?,
                    COMPLIANCE?, CORRELATION?, RESULT?)>
```

```
<!ATTLIST SERVICE
    severity CDATA #REQUIRED
    standard-severity CDATA #IMPLIED
    number CDATA #IMPLIED
>
<!-- VULNERABILITIES -->
<!ELEMENT VULNS (CAT)+>
<!ELEMENT VULN (TITLE, LAST_UPDATE?, CVSS_BASE?, CVSS_TEMPORAL?, PCI_FLAG,
               INSTANCE?, VENDOR_REFERENCE_LIST?, CVE_ID_LIST?,
               BUGTRAQ_ID_LIST?, DIAGNOSIS?, DIAGNOSIS_COMMENT?,
               CONSEQUENCE?, CONSEQUENCE_COMMENT?,
               SOLUTION?, SOLUTION_COMMENT?, COMPLIANCE?, CORRELATION?,
               RESULT?)>
<!-- number is Qualys numeric ID -->
<!-- cveid is the CVE identification code (if any) -->
<!-- severity is Qualys severity level 1 to 5 (possibly customized)  -->
<!-- standard-severity is the original Qualys severity level 1 to 5 if it
has been customized by the user -->
<!ATTLIST VULN
    number CDATA #REQUIRED
    cveid CDATA #IMPLIED
    severity CDATA #REQUIRED
    standard-severity CDATA #IMPLIED
>

<!-- Required Element -->

<!ELEMENT TITLE (#PCDATA)>

<!-- Optional Elements -->

<!ELEMENT LAST_UPDATE (#PCDATA)>

<!ELEMENT CVSS_BASE (#PCDATA)>
<!ATTLIST CVSS_BASE
    source CDATA #IMPLIED
>

<!ELEMENT CVSS_TEMPORAL (#PCDATA)>
<!ELEMENT PCI_FLAG (#PCDATA)>

<!ELEMENT VENDOR_REFERENCE_LIST (VENDOR_REFERENCE+)>
<!ELEMENT VENDOR_REFERENCE (ID,URL)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT URL (#PCDATA)>

<!ELEMENT CVE_ID_LIST (CVE_ID+)>
<!ELEMENT CVE_ID (ID,URL)>
```

```
<!ELEMENT BUGTRAQ_ID_LIST (BUGTRAQ_ID+)>
<!ELEMENT BUGTRAQ_ID (ID,URL)>

<!ELEMENT DIAGNOSIS (#PCDATA)>
<!ELEMENT DIAGNOSIS_COMMENT (#PCDATA)>
<!ELEMENT CONSEQUENCE (#PCDATA)>
<!ELEMENT CONSEQUENCE_COMMENT (#PCDATA)>
<!ELEMENT SOLUTION (#PCDATA)>
<!ELEMENT SOLUTION_COMMENT (#PCDATA)>

<!ELEMENT COMPLIANCE (COMPLIANCE_INFO+)>
<!ELEMENT COMPLIANCE_INFO (COMPLIANCE_TYPE, COMPLIANCE_SECTION,
                           COMPLIANCE_DESCRIPTION)>
<!ELEMENT COMPLIANCE_TYPE (#PCDATA)>
<!ELEMENT COMPLIANCE_SECTION (#PCDATA)>
<!ELEMENT COMPLIANCE_DESCRIPTION (#PCDATA)>

<!ELEMENT CORRELATION (EXPLOITABILITY?,MALWARE?)>
<!ELEMENT EXPLOITABILITY (EXPLT_SRC)+>
<!ELEMENT EXPLT_SRC (SRC_NAME, EXPLT_LIST)>
<!ELEMENT SRC_NAME (#PCDATA)>
<!ELEMENT EXPLT_LIST (EXPLT)+>
<!ELEMENT EXPLT (REF, DESC, LINK?)>
<!ELEMENT REF (#PCDATA)>
<!ELEMENT DESC (#PCDATA)>
<!ELEMENT LINK (#PCDATA)>

<!ELEMENT MALWARE (MW_SRC)+>
<!ELEMENT MW_SRC (SRC_NAME, MW_LIST)>
<!ELEMENT MW_LIST (MW_INFO)+>
<!ELEMENT MW_INFO (MW_ID, MW_TYPE?, MW_PLATFORM?, MW_ALIAS?, MW_RATING?,
                   MW_LINK?)>
<!ELEMENT MW_ID (#PCDATA)>
<!ELEMENT MW_TYPE (#PCDATA)>
<!ELEMENT MW_PLATFORM (#PCDATA)>
<!ELEMENT MW_ALIAS (#PCDATA)>
<!ELEMENT MW_RATING (#PCDATA)>
<!ELEMENT MW_LINK (#PCDATA)>

<!ELEMENT INSTANCE (#PCDATA)>

<!-- if format is set to "table" -->
<!-- tab '\t' is the col separator -->
<!-- and new line '\n' is the end of row -->
<!ELEMENT RESULT (#PCDATA)>
<!ATTLIST RESULT
    format CDATA #IMPLIED
>
```

```
<!-- SECURITY TIPS -->
<!ELEMENT PRACTICES (CAT+)>
<!ELEMENT PRACTICE (TITLE, LAST_UPDATE?, CVSS_BASE?, CVSS_TEMPORAL?,
                    PCI_FLAG, INSTANCE?, VENDOR_REFERENCE_LIST?,
                    CVE_ID_LIST?, BUGTRAQ_ID_LIST?,
                    DIAGNOSIS?, DIAGNOSIS_COMMENT?, CONSEQUENCE?,
                    CONSEQUENCE_COMMENT?, SOLUTION?, SOLUTION_COMMENT?,
                    COMPLIANCE?, CORRELATION?, RESULT?)>
<!ATTLIST PRACTICE
    number CDATA #REQUIRED
    cveid CDATA #IMPLIED
    severity CDATA #REQUIRED
    standard-severity CDATA #IMPLIED
>

<!-- EOF -->
```

XPaths for Vulnerability Scan Results

Header Information

HEADER and IP Elements

XPath	element specification / notes
/SCAN	((HEADER | ERROR | IP)+)
attribute: **value**	**value** is *required* and is the reference number for the scan
/SCAN/HEADER	(KEY+, ASSET_GROUPS?, ASSET_TAG_LIST?, OPTION_PROFILE?)
/SCAN/HEADER/KEY	(#PCDATA)
attribute: **value**	**value** is *implied* and, if present, will be one of the following: USERNAME.....The Qualys user login name for the user that initiated the scan request. COMPANY.....The company associated with the Qualys user. DATE.....The date when the scan was started. The date appears in YYYY-MM-DDTHH:MM:SSZ format (in UTC/GMT) like this: "2002-06-08T16:30:15Z" TITLE .....A descriptive title. When the user specifies a title for the scan request, the user-supplied title appears. When unspecified, a standard title is assigned. TARGET.....The host(s) specified for the scan target. EXCLUDED_TARGET.....The host(s) excluded from the scan. DURATION.....The time it took to complete the scan. SCAN_HOST .....The host name of the host that processed the scan. NBHOST_ALIVE.....The number of hosts found to be “alive.” NBHOST_TOTAL.....The total number of hosts. REPORT_TYPE.....The report type: “API” for an on-demand scan request launched from the API, “On-demand” for an on-demand scan launched from the Qualys user interface, and “Scheduled” for a scheduled task. OPTIONS.....The options settings in the options profile that was applied to the scan. Note the options information provided may be incomplete. DEFAULT_SCANNER.....The value 1 indicates that the default scanner was enabled for the scan. ISCANNER_NAME.....The scanner appliance name or “external” (for external scanner) used for the scan.

HEADER and IP Elements <body>(continued)

XPath	element specification / notes
/SCAN/HEADER/KEY	(#PCDATA)
attribute: **value**	STATUS..... The scan job status. QUEUED - A user launched the scan or the service started a scan based on a scan schedule. The scan job is waiting to be distributed to scanner(s). RUNNING - The scanner(s) are actively running the scan job. FINISHED - The scanner(s) have finished the scan job, the scan results were loaded onto the platform, and vulnerabilities were found. NOVULNSFOUND - The scanner(s) have finished the scan job, the scan results were loaded onto the platform, and no vulnerabilities were found. NOHOSTALIVE - The scanner(s) have finished the scan job, the scan results were loaded onto the platform, and target hosts were down (not alive). LOADING - The scanner(s) have finished the scan job, the scan results are being loaded onto the platform, and some scan results may be available. CANCELING - A user canceled the scan, and the scanner(s) are in the process of stopping the scan job. CANCELED - A user canceled the scan, the scanner(s) have stopped the scan job, and some scan results may be available. PAUSING - A user paused the scan, and the scanner(s) are in the process of stopping the scan. PAUSED - A user paused the scan, the scanner(s) stopped the scan job (segment), and some scan results may be available. RESUMING - A user resumed the scan, and the scanner(s) are starting to run the scan job (a new scan segment). ERROR - An error occurred during scan, and the scan did not complete. INTERRUPTED - The scan was interrupted and did not complete.
/SCAN/ERROR	(#PCDATA)
attribute: **number**	**number** is *implied* and, if present, is an error code
/SCAN/HEADER/ASSET_GROUPS (ASSET_GROUP+)	
/SCAN/HEADER/ASSET_GROUPS/ASSET_GROUP (ASSET_GROUP_TITLE)	
/SCAN/HEADER/ASSET_GROUPS/ASSET_GROUP/ASSET_GROUP_TITLE (#PCDATA)	
	The title of an asset group that was included in the scan target.
/SCAN/HEADER/OPTION_PROFILE (OPTION_PROFILE_TITLE)	
/SCAN/HEADER/OPTION_PROFILE/OPTION_PROFILE_TITLE (#PCDATA)	
	The title of the option profile that was applied to the scan.
attribute: **option_profile_default**	**option_profile_default** is *implied* and, if present, 1 means this option profile is the default in the user's account; 0 means it is not the default profile.
/SCAN/HEADER/ASSET_TAG_LIST (INCLUDED_TAGS, EXCLUDED_TAGS?)	
/SCAN/HEADER/ASSET_TAG_LIST/INCLUDED_TAGS/ASSET_TAG (#PCDATA)	
	The list of asset tags included in the scan target. The scope "all" means hosts matching all tags; scope "any" means hosts matching at least one of the tags.
/SCAN/HEADER/ASSET_TAG_LIST/EXCLUDED_TAGS/ASSET_TAG (#PCDATA)	
	The list of asset tags excluded from the scan target. The scope "all" means hosts matching all tags; scope "any" means hosts matching at least one of the tags.

HEADER and IP Elements <body>(continued)

XPath	element specification / notes
/SCAN/IP	(OS?, OS_CPE?, NETBIOS_HOSTNAME?, INFOS?, SERVICES?, VULNS?, PRACTICES?)
attribute: **value**	**value** is *required* and is an IP address
attribute: **name**	**name** is *implied* and, if present, is an Internet DNS host name
attribute: **status**	**status** is *implied* and, if present, will be one of the following: down.....The host was down (appears in live scan results only). Finish .....The scan finished (appears in live scan results only). no vuln .....No vulnerabilities were found on the host (appears in saved scan reports and live scan results). Note: The "down" or "Finish" element appears online in live scan results only, the results returned directly from the scanner. These elements are not present in saved scan reports, retrieved using the scan_report.php function.
/SCAN/IP/OS	(#PCDATA) The operating system name detected on the host.
/SCAN/IP/OS_CPE	(#PCDATA) The OS CPE name assigned to the operating system detected on the host. (The OS CPE name appears only when the OS CPE feature is enabled for the subscription, and an authenticated scan was run on this host after enabling this feature.)
/SCAN/IP/NETBIOS_HOSTNAME	(#PCDATA) The NetBIOS host name, when available.

Information Gathered

Information gathered vulnerabilities are grouped under the <INFOS> element.

INFOS Element

XPath	element specification / notes
/SCAN/IP/INFOS	(CAT)+
/SCAN/IP/INFOS/CAT	(INFO+) Note: When CAT is a child of INFOS, it can only contain INFO elements.
attribute: **value**	**value** is *required* and will be one vulnerability category name
attribute: **fqdn**	**fqdn** is *implied* and, if present, is the fully qualified Internet host name
attribute: **port**	**port** is *implied* and, if present, is the port number that the information gathered was detected on
attribute: **protocol**	**protocol** is *implied* and, if present, is the protocol used to detect the information gathered, such as TCP or UDP
attribute: **misc**	**misc** is *implied* and, if present, will be "over ssl," indicating the information gathered was detected using SSL

Services

Service vulnerabilities are grouped under the <SERVICES> element.

SERVICES Element

XPath	element specification / notes
/SCAN/IP/SERVICES	(CAT)+
/SCAN/IP/SERVICES/CAT	(SERVICE+) Note: When CAT is a child of SERVICES, it can only contain SERVICE elements.
attribute: **value**	**value** is *required* and will be one vulnerability category name
attribute: **fqdn**	**fqdn** is *implied* and, if present, is the fully qualified Internet host name
attribute: **port**	**port** is *implied* and, if present, is the port number that the service was detected on
attribute: **protocol**	**protocol** is *implied* and, if present, is the protocol used to detect the service, such as TCP or UDP
attribute: **misc**	**misc** is *implied* and, if present, will contain "over ssl," indicating the service was detected using SSL

Confirmed Vulnerabilities

Confirmed vulnerabilities are grouped under the <VULNS> element.

VULNS Element

XPath	element specifications / notes
/SCAN/IP/VULNS	(CAT)+
/SCAN/IP/VULNS/CAT	(VULN+) Note: When CAT is a child of VULNS, it can only contain VULN elements.
attribute: **value**	**value** is *required* and will be one vulnerability category name
attribute: **fqdn**	**fqdn** is *implied* and, if present, is the fully qualified Internet host name
attribute: **port**	**port** is *implied* and, if present, is the port number the confirmed vulnerability was detected on
attribute: **protocol**	**protocol** is *implied* and, if present, is the protocol used to detect the confirmed vulnerability, such as TCP or UDP
attribute: **misc**	**misc** is *implied* and, if present, will contain "over ssl," indicating the confirmed vulnerability was detected using SSL

Potential Vulnerabilities

Potential vulnerabilities are grouped under the <PRACTICES> element.

PRACTICES Element

XPath	element specifications / notes
/SCAN/IP/PRACTICES	(CAT)+
/SCAN/IP/PRACTICES/CAT	(PRACTICE+) Note: When CAT is a child of PRACTICES, it can only contain PRACTICE elements. A practice is a potential vulnerability.
attribute: **value**	**value** is *required* and will be one vulnerability category name
attribute: **fqdn**	**fqdn** is *implied* and, if present, is the fully qualified Internet host name
attribute: **port**	**port** is *implied* and, if present, is the port number that he potential vulnerability was detected on
attribute: **protocol**	**protocol** is *implied* and, if present, is the protocol used to detect the potential vulnerability, such as TCP or UDP
attribute: **misc**	**misc** is *implied* and, if present, will contain "over ssl," indicating the potential vulnerability was detected using SSL

Vulnerability Details

Vulnerability details are provided for each detected vulnerability using the vulnerability elements. The details for each vulnerability instance appear under grouping and category elements: confirmed vulnerability (VULNS/CAT/VULN), potential vulnerability (PRACTICES/CAT/PRACTICE), information gathered (INFOS/CAT/INFO), and service (SERVICES/CAT/SERVICE).

Vulnerability Details Element

XPath	element specifications / notes
/SCAN/IP/VULNS/CAT/vulnerability_element	
	(TITLE, LAST_UPDATE, CVSS_BASE?, CVSS_TEMPORAL?, PCI_FLAG, INSTANCE?, VENDOR_REFERENCE_LIST?, CVE_ID_LIST, BUGTRAQ_ID_LIST?, DIAGNOSIS?, DIAGNOSIS_COMMENT?, CONSEQUENCE?, CONSEQUENCE?_COMMENT, SOLUTION?, SOLUTION_COMMENT?, COMPLIANCE?, CORRELATION?, RESULT?)
	The vulnerability element, where the variable "vulnerability_elements" represents a vulnerability element grouping: VULNS for confirmed vulnerabilities, PRACTICES for potential vulnerabilities, INFOS for information gathered, or SERVICES for services. The variable "vulnerability_element" represents a vulnerability element for a single vulnerability instance: VULN for confirmed vulnerability, PRACTICE for potential vulnerability, INFO for information gathered, or SERVICE for service.
attribute: **number**	**number** is *required* and is the Qualys ID number assigned to the vulnerability
attribute: **cveid**	**cveid** is *implied* and, if present, is the CVE ID (name) for the vulnerability
attribute: **severity**	**severity** is *required* and is the severity level assigned to the vulnerability, an integer between 1 and 5
attribute: **standard-severity**	**standard-severity** is *implied* and, if present, is the standard severity level assigned to the vulnerability by Qualys, an integer between 1 and 5
/SCAN/IP/VULNS/CAT/vulnerability_element/TITLE (#PCDATA)	
	The title of the vulnerability, from the Qualys KnowledgeBase.
/SCAN/IP/VULNS/CAT/vulnerability_element/LAST_UPDATE (#PCDATA)	
	The date and time when the vulnerability was last updated in the Qualys KnowledgeBase, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/SCAN/IP/VULNS/CAT/vulnerability_element/CVSS_BASE (#PCDATA)	
	The CVSS base score assigned to the vulnerability.
attribute: **source**	Note: This attribute is never present in XML output for this release.
/SCAN/IP/VULNS/CAT/vulnerability_element/CVSS_TEMPORAL (#PCDATA)	
	The CVSS temporal score assigned to the vulnerability.

Vulnerability Details Element <body>(continued)

XPath	element specifications / notes
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/PCI_FLAG (#PCDATA)	
	A flag indicating whether this vulnerability must be fixed to pass a PCI compliance scan. This information helps users to determine whether the vulnerability must be fixed to meet PCI compliance goals, without having to run additional PCI compliance scans. The value 1 is returned when the vulnerability must be fixed to pass PCI compliance; the value 0 is returned when the vulnerability does not need to be fixed to pass PCI compliance.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/DIAGNOSIS (#PCDATA)	
	The Qualys provided description of the threat.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/DIAGNOSIS_COMMENT (#PCDATA)	
	User-defined description of the threat, if any
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CONSEQUENCE (#PCDATA)	
	The Qualys provided description of the impact.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CONSEQUENCE_COMMENT (#PCDATA)	
	User-defined description of the impact, if any.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/SOLUTION (#PCDATA)	
	The Qualys provided description of the solution. When virtual patch information is correlated with a vulnerability, the virtual patch information from Trend Micro appears under the heading “Virtual Patches:”. This includes a list of virtual patches and a link to more information.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/SOLUTION_COMMENT (#PCDATA)	
	User-defined description of the solution, if any.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/COMPLIANCE (COMPLIANCE_INFO+)	
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/COMPLIANCE/COMPLIANCE_INFO	
	(COMPLIANCE_TYPE, COMPLIANCE_SECTION, COMPLIANCE_DESCRIPTION)
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/COMPLIANCE/COMPLIANCE_INFO/ COMPLIANCE_TYPE (#PCDATA)	
	The type of a compliance policy or regulation that is associated with the vulnerability. A valid value is: -HIPAA (Health Insurance Portability and Accountability Act) -GLBA (Gramm-Leach-Bliley Act) -CobIT (Control Objectives for Information and related Technology -SOX (Sarbanes-Oxley Act)
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/COMPLIANCE/COMPLIANCE_INFO/ COMPLIANCE_SECTION (#PCDATA	
	The section of a compliance policy or regulation associated with the vulnerability.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/COMPLIANCE/COMPLIANCE_INFO/ COMPLIANCE_DESCRIPTION (#PCDATA)	
	The description of a compliance policy or regulation associated with the vulnerability.

Vulnerability Details Element <body>(continued)

XPath	element specifications / notes
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION (EXPLOITABILITY?, MALWARE?)	
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/EXPLOITABILITY (EXPLT_SRC)+	
	The <EXPLOITABILITY> element and its sub-elements appear only when there is exploitability information for the vulnerability from third party vendors and/or publicly available sources.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/EXPLOITABILITY/ EXPLT_SRC (SRC_NAME, EXPLT_LIST)	
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/EXPLOITABILITY/ EXPLT_SRC/SRC_NAME (#PCDATA)	
	The name of a third party vendor or publicly available source of the vulnerability information.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/EXPLOITABILITY/ EXPLT_SRC/EXPLT_LIST (EXPLT)+	
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/EXPLOITABILITY/ EXPLT_SRC/EXPLT_LIST/EXPLT (REF, DESC, LINK?)	
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/EXPLOITABILITY/ EXPLT_SRC/EXPLT_LIST/EXPLT/REF (#PCDATA)	
	The CVE reference for the exploitability information.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/EXPLOITABILITY/ EXPLT_SRC/EXPLT_LIST/EXPLT/DESC (#PCDATA)	
	The description provided by the source of the exploitability information (third party vendor or publicly available source).
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/EXPLOITABILITY/ EXPLT_SRC/EXPLT_LIST/EXPLT/LINK (#PCDATA)	
	A link to the exploit, when available.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/MALWARE (MW_SRC)+	
	The <MALWARE> element and its sub-elements appear only when there is malware information for the vulnerability from Trend Micro.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/MALWARE/ MW_SRC (SRC_NAME, MW_LIST)	
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/MALWARE/ MW_SRC/SRC_NAME (#PCDATA)	
	The name of the source of the malware information: Trend Micro.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/MALWARE/ MW_SRC/MW_LIST (MW_INFO)+	
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/MALWARE/ MW_SRC/MW_LIST/MW_INFO	(MW_ID, MW_TYPE?, MW_PLATFORM?, MW_ALIAS?, MW_RATING?, MW_LINK?)
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/MALWARE/ MW_SRC/MW_LIST/MW_INFO /MW_ID (#PCDATA)	
	The malware name/ID assigned by Trend Micro.

Vulnerability Details Element <body>(continued)

XPath	element specifications / notes
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_TYPE (#PCDATA)	
	The type of malware, such as Backdoor, Virus, Worm or Trojan.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_PLATFORM (#PCDATA)	
	A list of the platforms that may be affected by the malware.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_ALIAS (#PCDATA)	
	A list of other names used by different vendors and/or publicly available sources to refer to the same threat.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_RATING (#PCDATA)	
	The overall risk rating as determined by Trend Micro: Low, Medium or High.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_LINK (#PCDATA)	
	A link to malware details.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/INSTANCE (#PCDATA)	
	The Oracle DB instance the vulnerability was deteccted on.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/RESULT (#PCDATA)	
	Specific scan test results for the vulnerability, from the host assessment data.
attribute: **format**	**format** is *implied* and, if present, will be "table" to indicate that the results are a table that has columns separated by tabulation characters and rows separated by new-line characters
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/VENDOR_REFERENCE_LIST	
	(VENDOR_REFERENCE+)
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/VENDOR_REFERENCE_LIST/VENDOR_REFERENCE (ID, URL)	
	The name of a vendor reference, and the URL to this vendor reference.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/reference_list/reference/ID (#PCDATA)	
	The name of a vendor reference, CVE name, or Bugtraq ID.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/reference_list/reference/URL (#PCDATA)	
	The URL to the vendor reference, CVE name, or Bugtraq ID.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CVE_ID_LIST	
	(CVE_ID+)

Vulnerability Details Element <body>(continued)

XPath	element specifications / notes
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CVE_ID_LIST/CVE_ID	
	(ID, URL)
	A CVE name assigned to the vulnerability, and the URL to this CVE name. CVE (Common Vulnerabilities and Exposures) is a list of common names for publicly known vulnerabilities and exposures. Through open and collaborative discussions, the CVE Editorial Board determines which vulnerabilities or exposures are included in CVE. If the CVE name starts with CAN (candidate) then it is under consideration for entry into CVE.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/BUGTRAQ_LIST	
	(BUGTRAQ_ID+)
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/BUGTRAQ_LIST/BUGTRAQ_ID	
	(ID, URL)
	A Bugtraq ID assigned to the vulnerability, and the URL to this Bugtraq ID.

Live and Saved Scan Results

Live scan results are the results returned directly from the scanner. The live scan results provide a status indicator for each host in the <IP> section. When the scan results are saved on the Qualys server, the report may be viewed using the **scan_report.php** function or the Qualys user interface.

XML Header Response for Saved Scan Results

Once a **scan_report.php** API request is made for saved scan results, the service immediately sends an XML header response as shown below:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCAN SYSTEM "https://qualysapi.qualys.com/
scan-1.dtd">
<! -- Initializing Data -- >
<!-- Generating XML report -->
<SCAN value="scan/XXXXXX">
```

where <qualysapi.qualys.com> is the API server where your account is located.

The API response is sent right away while waiting for the scan data to be processed. This immediate response is very helpful for customers with large scan results.

Scan Results with Vulnerabilities Detected

In the case where vulnerabilities were detected during a scan, the service returns live scan results including the full vulnerability assessment details.

At the completion of a scan, the live scan results include the "Finish" status in the <IP> tag:

```
<IP value="194.55.109.7" name="tiger.corp.us.com"
status="Finish">
```

In the saved scan report returned by the **scan_report.php** function, the <IP> tag appears without the "status" attribute like this:

```
<IP value="194.55.109.7" name="tiger.corp.us.com">
```

Scan Results with No Vulnerabilities Detected

If the target was scanned and no vulnerabilities were found, the live scan results include scan summary information and the "no vuln" status as shown in the sample below. This status may be returned due to one or more of these reasons: there was no data found for the host(s), the host(s) were never scanned, the data for the host(s) was purged. The "no vuln" status appears in live and saved scan reports.

```
<?xml version="1.0" encoding="UTF-8" ?>
  <!DOCTYPE SCAN (View Source for full doctype...)>
- <!--  scan is running on 194.55.110.29
  -->
- <SCAN value="scan/nnnnnnnnnn.nnnnn">
- <!--  keep-alive
  -->
  <IP value="197.45.100.53" status="no vuln" />

<HEADER>
  <KEY value="USERNAME">user_name</KEY>
  <KEY value="COMPANY"><![CDATA[company_name]]></KEY>
  <KEY value="DATE">2005-11-08T17:36:53Z</KEY>
  <KEY value="TITLE"><![CDATA[Vulnerability analysis on
197.45.100.53]]</KEY>
  <KEY value="TARGET">197.45.100.53</KEY>
  <KEY value="DURATION">00:02:30</KEY>
  <KEY value="SCAN_HOST">hostname (Scanner version, Web version, Vulnsigs
version)</KEY>
  <KEY value="NBHOST_ALIVE">1</KEY>
  <KEY value="NBHOST_TOTAL">1</KEY>
  <KEY value="REPORT_TYPE">API (default option profile)</KEY>
  <KEY value="OPTIONS">option settings</KEY>
```

```
  <KEY value="ISCANNER_NAME">scanner_appliance_name</KEY>
  <KEY value="STATUS">NOVULNSFOUND</KEY>
  <OPTION_PROFILE>
    <OPTION_PROFILE_TITLE option_profile_default="1"><![CDATA[Initial
Options]]></OPTION_PROFILE_TITLE>
  </OPTION_PROFILE>
</HEADER>
</SCAN>
```

Scan reports with no vulnerabilities found that are saved on the Qualys server may be viewed using the **scan_report.php** function or the Qualys user interface.

Empty Scan Results

The service returns empty scan results if the target hosts were down (not alive), or if a scan was cancelled or interrupted before a single host was scanned. Empty results include scan summary information plus the "down" status as shown in the sample below (variables appear in italics). The "down" status appears in live and saved scan reports.

```
<?xml version="1.0" encoding="UTF-8" ?>
...
- <SCAN value="scan/nnnnnnnnn.nnnnn">
 <IP value="194.55.110.29" status="down" />
  <ERROR number="3509">No host alive</ERROR>
 <HEADER>
  <KEY value="USERNAME">user_name</KEY>
  <KEY value="COMPANY"><![CDATA[company_name]]></KEY>
  <KEY value="DATE">2005-11-30T00:19:03Z</KEY>
...
</HEADER>
</SCAN>
```

Empty scan results that are saved on the Qualys server may be viewed using the **scan_report.php** function or the Qualys user interface.

Scan Report List

The scan report list is returned from the **scan_report_list.php** function. All saved scans for the user account are listed.

The scan report list DTD and XPaths are described below.

DTD for Scan Report List

A recent DTD for the scan report list (scan_report_list.dtd) is shown below.

```
<!-- QUALYS SCAN_REPORT_LIST DTD -->

<!ELEMENT SCAN_REPORT_LIST (ERROR|(SCAN_REPORT*))>
<!ATTLIST SCAN_REPORT_LIST
    user CDATA #REQUIRED
    from CDATA #REQUIRED
    to CDATA #REQUIRED
    with_target CDATA #IMPLIED
>
<!ELEMENT SCAN_REPORT (ASSET_GROUPS?, OPTION_PROFILE?)>
<!ATTLIST SCAN_REPORT
    ref CDATA #REQUIRED
    date CDATA #REQUIRED
    target CDATA #REQUIRED
    status CDATA #IMPLIED
>

<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR
    number CDATA   #IMPLIED
>

<!ELEMENT ASSET_GROUP (ASSET_GROUP_TITLE)>
<!ELEMENT ASSET_GROUPS (ASSET_GROUP*)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>
<!ELEMENT OPTION_PROFILE (OPTION_PROFILE_TITLE)>
<!ELEMENT OPTION_PROFILE_TITLE (#PCDATA)>
<!ATTLIST OPTION_PROFILE_TITLE
    option_profile_default CDATA   #IMPLIED
>

<!-- EOF -->
```

XPaths for Scan Report List

This section describes the XPaths for the scan report list.

XPath	element specification / notes
/SCAN_REPORT_LIST	(ERROR | (SCAN_REPORT*))
attribute: **user**	**user** is *required* and is the Qualys user name
attribute: **from**	**from** is *required* and is the oldest date in the range of available scans. The date appears in YYYY-MM-DDTHH:MM:SSZ format (in UTC/GMT) like this: "2002-06-08T16:30:15Z"
attribute: **to**	**to** is *required* and is the newest date in the range of available scans. The date appears in YYYY-MM-DDTHH:MM:SSZ format (in UTC/GMT) like this: "2002-06-08T16:30:15Z"
attribute: **with_target**	**with_target** is *implied* and, if present, is an IP address that will be found in each of the reports in the list
/SCAN_REPORT_LIST/SCAN_REPORT (ASSET_GROUPS?, OPTION_PROFILE?	
attribute: **ref**	**ref** is *required* and is the scan reference
attribute: **date**	**date** is *required* and is the date when the scan was performed. The date appears in YYYY-MM-DDTHH:MM:SSZ format (in UTC/GMT) like this: "2002-06-08T16:30:15Z"
attribute: **target**	**target** is *required* and is the IP address (or range of IP addresses) upon which the scan was performed
attribute: **status**	**status** is *implied* and, if present, is the job status of the scan. QUEUED - A user launched the scan or the service started a scan based on a scan schedule. The scan job is waiting to be distributed to scanner(s). RUNNING - The scanner(s) are actively running the scan job. FINISHED - The scanner(s) have finished the scan job, the scan results were loaded onto the platform, and vulnerabilities were found. NOVULNSFOUND - The scanner(s) have finished the scan job, the scan results were loaded onto the platform, and no vulnerabilities were found. NOHOSTALIVE - The scanner(s) have finished the scan job, the scan results were loaded onto the platform, and target hosts were down (not alive). LOADING - The scanner(s) have finished the scan job, the scan results are being loaded onto the platform, and some scan results may be available. CANCELING - A user canceled the scan, and the scanner(s) are in the process of stopping the scan job. CANCELED - A user canceled the scan, the scanner(s) have stopped the scan job, and some scan results may be available. PAUSING - A user paused the scan, and the scanner(s) are in the process of stopping the scan. PAUSED - A user paused the scan, the scanner(s) stopped the scan job (segment), and some scan results may be available. RESUMING - A user resumed the scan, and the scanner(s) are starting to run the scan job (a new scan segment). ERROR - An error occurred during scan, and the scan did not complete. INTERRUPTED - The scan was interrupted and did not complete.
/SCAN_REPORT_LIST/SCAN_REPORT/ASSET_GROUPS (ASSET_GROUP+)	
/SCAN_REPORT_LIST/SCAN_REPORT/ASSET_GROUPS/ASSET_GROUP (ASSET_GROUP_TITLE)	

XPath	element specification / notes
/SCAN_REPORT_LIST/SCAN_REPORT/ASSET_GROUPS/ASSET_GROUP/ASSET_GROUP_TITLE (#PCDATA)	
	The title of an asset group that was included in the scan target.
/SCAN_REPORT_LIST/SCAN_REPORT/OPTION_PROFILE (OPTION_PROFILE_TITLE)	
/SCAN_REPORT_LIST/SCAN_REPORT/OPTION_PROFILE/OPTION_PROFILE_TITLE (#PCDATA)	
	The title of the option profile, as defined in the Qualys user interface, that was applied to the scan.
attribute: **option_profile_default**	**option_profile_default** is *implied* and, if present, is a code that specifies whether the option profile was defined as the default option profile in the API user's account. A value of 1 is returned when this option profile is the default. A value of 0 is returned when this option profile is not the default.
/SCAN_REPORT/ERROR	(#PCDATA)
attribute: **number**	**number** is *implied* and, if present, is an error code

Running Scans and Maps List

The running tasks list is returned from the **scan_running_list.php** function. All running tasks in the user account are listed.

The running tasks list DTD and XPaths are described below.

DTD for Running Scans and Maps List

A recent DTD for the running scans and maps list (scan_running_list.dtd) is below.

```
<!-- QUALYS SCAN_RUNNING_LIST DTD -->
<!ELEMENT SCAN_RUNNING_LIST (SCAN*,ERROR*)>
<!-- "at" attribute is the current platform date and time -->
<!ATTLIST SCAN_RUNNING_LIST
          username CDATA #REQUIRED
          at CDATA #REQUIRED>
<!-- value is the reference of the scan -->
<!ELEMENT SCAN (KEY+, ASSET_GROUPS?,  OPTION_PROFILE+)>
<!ATTLIST SCAN
          value CDATA #REQUIRED
<!-- some information about the running scan -->
<!ELEMENT KEY (#PCDATA)*>
<!ATTLIST KEY
          value CDATA #IMPLIED>

<!ELEMENT ERROR (#PCDATA)*>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!ELEMENT ASSET_GROUP (ASSET_GROUP_TITLE)>
<!ELEMENT ASSET_GROUPS (ASSET_GROUP+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>
<!ELEMENT OPTION_PROFILE (OPTION_PROFILE_TITLE)>
<!ELEMENT OPTION_PROFILE_TITLE (#PCDATA)>
<!ATTLIST OPTION_PROFILE_TITLE
    option_profile_default CDATA #IMPLIED
>
<!-- EOF -->
```

XPaths for Running Scans and Maps List

This section describes the XPaths in the XML running scans and maps list.

XPath	element specifications / notes
/SCAN_RUNNING_LIST	(SCAN*,ERROR*)
attribute: **username**	**username** is *required* and is the Qualys user name
attribute: **at**	**at** is *required* and is the start timestamp of the longest running map or scan in the running scans and maps list. The timestamp appears in YYYY-MM-DDTHH:MM:SSZ format (in UTC/GMT) like this: "2003-09-08T16:30:15Z"
/SCAN_RUNNING_LIST/SCAN	(KEY+, ASSET_GROUPS?, OPTION_PROFILE+)
attribute: **value**	**value** is *required* and is the reference, or key, for the scan as follows: scan/nn .....The reference number for a scan (IP/Group). map/nn .....The reference number for a network map.
/SCAN_RUNNING_LIST/SCAN/KEY	(#PCDATA)*
attribute: **value**	**value** is *implied* and, if present, will be one of the following: type .....The type is either “scan” or “map”. target.....The target for a scan identifies IPs; the target for a map is a domain. nbhost_already_scanned .....The number of hosts already scanned. startdate.....The start timestamp of the scan or map. The timestamp appears in YYYY-MM-DDTHH:MM:SSZ format (in UTC/GMT) like this: "2002-06-08T16:30:15Z" scheduled .....Valid value is “true” for a scheduled task and “false” for an on-demand task. status.....The job status. One of RUNNING, FINISHED, LOADING, CANCELED, NOHOSTALIVE, NOVULNSFOUND (scan only). For a paused scan, PAUSED (scan in paused state). See the SCAN/HEADER/KEY status attribute in “Scan Results” for a description of each status.
/SCAN_RUNNING_LIST/ERROR	
attribute: **number**	**number** is *implied* and, if present, will be an error code
/SCAN_RUNNING_LIST/ASSET_GROUPS	(ASSET_GROUP+)
/SCAN_RUNNING_LIST/ASSET_GROUPS/ASSET_GROUP	(ASSET_GROUP_TITLE)
/SCAN_RUNNING_LIST/ASSET_GROUPS/ASSET_GROUP/ASSET_GROUP_TITLE	(#PCDATA)
	The title of an asset group that was specified as a scan or map target.

XPath	element specifications / notes
/SCAN_RUNNING_LIST/OPTION_PROFILE (OPTION_PROFILE_TITLE)	
/SCAN_RUNNING_LIST/OPTION_PROFILE/OPTION_PROFILE_TITLE (#PCDATA)	
	The title of the option profile that was applied to the scan or map.
attribute: **option_profile_default**	**option_profile_default** is *implied* and, if present, is a code that specifies whether the option profile was defined as the default in the user account. A value of 1 is returned when this option profile is the default. A value of 0 is returned when this option profile is not the default.

Scan Target History Output

The scan target history output is an XML report returned from the **scan_target_history.php** function. The report allows users to check whether a given set of IP addresses were included as targets for scans launched during a particular period of time.

The scan target history output DTD and XPaths are described below.

DTD for Scan History Output

A recent DTD for the scan target history output (scan_target_history_output.dtd) is below.

```
<!-- QUALYS SCAN TARGET HISTORY OUTPUT DTD -->

<!ELEMENT SCAN_TARGET_HISTORY_OUTPUT (ERROR | (HEADER, IP_TARGETED_LIST?,
                                      IP_NOT_TARGETED_LIST?))>

<!ELEMENT ERROR (#PCDATA)*>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!-- HEADER -->
<!ELEMENT HEADER (USER_LOGIN, COMPANY, DATETIME, WHERE)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT COMPANY (#PCDATA)>
<!ELEMENT DATETIME (#PCDATA)>

<!ELEMENT WHERE (DATE_FROM, DATE_TO, IPS?, ASSET_GROUP?,
                 FILTER_OPTION_PROFILE_TITLE?, DETAILED_HISTORY?,
                 IP_TARGETED_FLAG?, IP_NOT_TARGETED_FLAG?)>
<!ELEMENT DATE_FROM (#PCDATA)>
<!ELEMENT DATE_TO (#PCDATA)>
<!ELEMENT IPS (#PCDATA)>
<!ELEMENT ASSET_GROUP (#PCDATA)>
<!ELEMENT FILTER_OPTION_PROFILE_TITLE (#PCDATA)>
<!ATTLIST FILTER_OPTION_PROFILE_TITLE criterion CDATA #IMPLIED>
<!ELEMENT DETAILED_HISTORY (#PCDATA)>
<!ELEMENT IP_TARGETED_FLAG (#PCDATA)>
<!ELEMENT IP_NOT_TARGETED_FLAG (#PCDATA)>

<!-- TARGETED LIST -->
<!ELEMENT IP_TARGETED_LIST (IP_TARGETED*)>
<!ELEMENT IP_TARGETED (IP, NB_SCANS, IP_DETAILED_HISTORY?)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT NB_SCANS (#PCDATA)>
```

```
<!ELEMENT IP_DETAILED_HISTORY (SCAN*)>
<!ELEMENT SCAN (DATE, STATUS, REF, SCAN_TYPE, SCAN_TITLE,
                OPTION_PROFILE_TITLE?, DELETED?)>
<!ELEMENT DATE (#PCDATA)>
<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT REF (#PCDATA)>
<!ELEMENT SCAN_TYPE (#PCDATA)>
<!ELEMENT SCAN_TITLE (#PCDATA)>
<!ELEMENT OPTION_PROFILE_TITLE (#PCDATA)>
<!ELEMENT DELETED (#PCDATA)>

<!-- NOT TARGETED LIST -->
<!ELEMENT IP_NOT_TARGETED_LIST (RANGE*)>
<!ELEMENT RANGE (START, END)>
<!ELEMENT START (#PCDATA)>
<!ELEMENT END (#PCDATA)>
```

XPaths for Scan Target History Output

This section describes the XPaths in the scan target history output.

Scan Target History Output — Header Information

XPath	element specifications / notes
/SCAN_TARGET_HISTORY_OUTPUT	
	(ERROR | (HEADER, IP_TARGETED_LIST?, IP_NOT_TARGETED_LIST?))
/SCAN_TARGET_HISTORY_OUTPUT/ERROR (#PCDATA)	
attribute: **number**	**number** is *implied* and, if present, is an error code.
/SCAN_TARGET_HISTORY_OUTPUT/HEADER	
	(USER_LOGIN, COMPANY, DATETIME, WHERE)
/SCAN_TARGET_HISTORY_OUTPUT/HEADER/USER_LOGIN (#PCDATA)	
	The Qualys user login name for the user who made the scan target history request.
/SCAN_TARGET_HISTORY_OUTPUT/HEADER/COMPANY (#PCDATA)	
	The company associated with the Qualys user who made the API request.
/SCAN_TARGET_HISTORY_OUTPUT/HEADER/DATETIME (#PCDATA)	
	The date and time of the API request. The date appears in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/SCAN_TARGET_HISTORY_OUTPUT/HEADER/WHERE	
	(DATE_FROM, DATE_TO, IPS?, ASSET_GROUP?, FILTER_OPTION_PROFILE_TITLE?, DETAILED_HISTORY?, IP_TARGETED_FLAG?, IP_NOT_TARGETED_FLAG?)
	The WHERE element describes the input attributes specified with the scan_target_history.php request.

XPath	element specifications / notes
/SCAN_TARGET_HISTORY_OUTPUT/HEADER/WHERE/DATE_FROM (#PCDATA)	
	The start date/time, in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), of the time period representing the scope of the scan target history.
/SCAN_TARGET_HISTORY_OUTPUT/HEADER/WHERE/DATE_TO (#PCDATA)	
	The end date/time, in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), of the time period representing the scope of scan target history. If not specified by the user, the service sets this value to the date/time of the API request.
/SCAN_TARGET_HISTORY_OUTPUT/HEADER/WHERE/IPS (#PCDATA)	
	The specified IP addresses and/or ranges.
/SCAN_TARGET_HISTORY_OUTPUT/HEADER/ASSET_GROUP (#PCDATA)	
	The specified title of a target asset group including IP addresses.
/SCAN_TARGET_HISTORY_OUTPUT/HEADER/WHERE/FILTER_OPTION_PROFILE_TITLE (#PCDATA)	
	The text string used to filter scan data based on option profile title. The filter is defined by the text string and a prefix.
attribute: **criterion**	**number** is *implied* and, if present, indicates the match prefix: begin, match, contain, or end.
/SCAN_TARGET_HISTORY_OUTPUT/HEADER/WHERE/DETAILED_HISTORY (#PCDATA)	
	A flag indicating whether the output includes detailed history for IPs that were targeted (i.e. included the target for scans). The value 1 indicates detailed history is included.
/SCAN_TARGET_HISTORY_OUTPUT/HEADER/WHERE/IP_TARGETED_FLAG (#PCDATA)	
	A flag indicating whether the output includes information on IPs that were targeted (i.e. included in the target for scans). The value 1 indicates that IPs targeted are included.
/SCAN_TARGET_HISTORY_OUTPUT/HEADER/WHERE/IP_NOT_TARGETED_FLAG (#PCDATA)	
	A flag indicating whether the output includes information on IPs that were not targeted (i.e. not included in the target for scans). The value 1 indicates that IPs not targeted are included.

Scan Target History Output — IP Targeted List

XPath	element specifications / notes
/SCAN_TARGET_HISTORY_OUTPUT/IP_TARGETED_LIST (IP_TARGETED*)	
/SCAN_TARGET_HISTORY_OUTPUT/IP_TARGETED_LIST/IP_TARGETED	(IP, NB_SCANS, IP_DETAILED_HISTORY?)
/SCAN_TARGET_HISTORY_OUTPUT/IP_TARGETED_LIST/IP_TARGETED/IP (#PCDATA)	The IP address of a host that was scanned.
/SCAN_TARGET_HISTORY_OUTPUT/IP_TARGETED_LIST/IP_TARGETED/NB_SCANS (#PCDATA)	The number of scans found to have the IP address in the scan target.
/SCAN_TARGET_HISTORY_OUTPUT/IP_TARGETED_LIST/IP_TARGETED/IP_DETAILED_HISTORY (SCAN*)	This element is included only when the "detailed_history=1" attribute was specified for the API request. The sub-elements provide detailed history data on IPs targeted.
/SCAN_TARGET_HISTORY_OUTPUT/IP_TARGETED_LIST/IP_TARGETED/IP_DETAILED_HISTORY/SCAN	(DATE, STATUS, REF, SCAN_TYPE, SCAN_TITLE, OPTION_PROFILE_TITLE?, DELETED?)
/SCAN_TARGET_HISTORY_OUTPUT/IP_TARGETED_LIST/IP_TARGETED/IP_DETAILED_HISTORY/SCAN/DATE (#PCDATA)	The date/time when the scan was launched on the IP address, in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
/SCAN_TARGET_HISTORY_OUTPUT/IP_TARGETED_LIST/IP_TARGETED/IP_DETAILED_HISTORY/SCAN/STATUS (#PCDATA)	The status of the scan task on the IP address at the time of the request. Possible values are: FINISHED — Scan finished with vulnerabilities detected. NOVULNSFOUND — Scan finished with no vulnerabilities detected. NOHOSTALIVE — Scan finished with no hosts alive. CANCELED — Scan was canceled and did not complete. INTERRUPTED — Scan was interrupted and did not complete.
/SCAN_TARGET_HISTORY_OUTPUT/IP_TARGETED_LIST/IP_TARGETED/IP_DETAILED_HISTORY/SCAN/REF (#PCDATA)	The Qualys scan reference code assigned to the scan on the IP address.
/SCAN_TARGET_HISTORY_OUTPUT/IP_TARGETED_LIST/IP_TARGETED/IP_DETAILED_HISTORY/SCAN/SCAN_TYPE (#PCDATA)	The Qualys scan type: "ON-DEMAND" for an on demand scan launched from the Qualys user interface, "SCHEDULED" for a scheduled scan, and "API" for a scan request launched from the Qualys API.
/SCAN_TARGET_HISTORY_OUTPUT/IP_TARGETED_LIST/IP_TARGETED/IP_DETAILED_HISTORY/SCAN/SCAN_TITLE (#PCDATA)	A descriptive scan title. When the user specifies a title for the scan request, the user-supplied title appears. When unspecified, a standard title is assigned.

XPath	element specifications / notes
/SCAN_TARGET_HISTORY_OUTPUT/IP_TARGETED_LIST/IP_TARGETED/IP_DETAILED_HISTORY/SCAN/OPTION_PROFILE_TITLE (#PCDATA)	
	The title of the option profile applied to the scan on the IP address. If the scan results were deleted, then the option profile title is not available and thus not reported.
/SCAN_TARGET_HISTORY_OUTPUT/IP_TARGETED_LIST/IP_TARGETED/IP_DETAILED_HISTORY/SCAN/DELETED (#PCDATA)	
	A flag indicating whether the scan results were deleted. The value 1 indicates that scan results were deleted for the scan on the IP address.

Scan Target History Output — IP Not Targeted List

XPath	element specifications / notes
/SCAN_TARGET_HISTORY_OUTPUT/IP_NOT_TARGETED_LIST (RANGE*)	
/SCAN_TARGET_HISTORY_OUTPUT/IP_NOT_TARGETED_LIST/RANGE (START, END)	
	The RANGE elements identify the IP addresses that were not targeted (i.e. not included in the target for scans). IP addresses are returned in ranges. For a single IP not in a range, the start and end IPs are the same.
/SCAN_TARGET_HISTORY_OUTPUT/IP_NOT_TARGETED_LIST/RANGE/START (#PCDATA)	
	The start IP address.
/SCAN_TARGET_HISTORY_OUTPUT/IP_NOT_TARGETED_LIST/RANGE/END (#PCDATA)	
	The end IP address.

KnowledgeBase Download Output

The KnowledgeBase download output is an XML report returned from the **`knowledgebase_download.php`** function. This includes vulnerability data from the Qualys KnowledgeBase.

The KnowledgeBase download output DTD and XPaths are described below.

DTD for KnowledgeBase Download Output

A recent DTD for the KnowledgeBase download output (knowledgebase_download.dtd) is below.

```
<!-- QUALYS KNOWLEDGEBASE DOWNLOAD DTD -->

<!-- ===== VULNERABILITY INFORMATION ===== -->

<!ELEMENT VULNS (ERROR | (VULN)+)>

<!-- Error Information -->
<!ELEMENT ERROR (#PCDATA) >
<!ATTLIST ERROR number CDATA #IMPLIED >

<!ELEMENT VULN (QID, VULN_TYPE, SEVERITY_LEVEL, TITLE, CATEGORY?,
                LAST_UPDATE?, BUGTRAQ_ID_LIST?, PATCHABLE,
                VENDOR_REFERENCE_LIST?, CVE_ID_LIST?,
                DIAGNOSIS?, CONSEQUENCE?, SOLUTION?, COMPLIANCE?,
                CORRELATION?, CVSS_BASE?, CVSS_TEMPORAL?,
                CVSS_ACCESS_VECTOR?, CVSS_ACCESS_COMPLEXITY?,
                CVSS_AUTHENTICATION?, CVSS_CONFIDENTIALITY_IMPACT?,
                CVSS_INTEGRITY_IMPACT?, CVSS_AVAILABILITY_IMPACT?,
                CVSS_EXPLOITABILITY?, CVSS_REMEDIATION_LEVEL?,
                CVSS_REPORT_CONFIDENCE?, PCI_FLAG?, PCI_REASONS?)>

<!-- Required Elements -->
<!ELEMENT QID (#PCDATA)>
<!ELEMENT VULN_TYPE (#PCDATA)> <!-- Vulnerability | Potential
Vulnerability | Vulnerability or Potential Vulnerability | Information
Gathered  -->
<!ELEMENT SEVERITY_LEVEL (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>

<!-- Optional Elements -->
<!ELEMENT CATEGORY (#PCDATA)>
<!ELEMENT LAST_UPDATE (#PCDATA)>

<!ELEMENT BUGTRAQ_ID_LIST (BUGTRAQ_ID)+>
<!ELEMENT BUGTRAQ_ID (ID,URL)>
```

```
<!ELEMENT ID (#PCDATA)>
<!ELEMENT URL (#PCDATA)>

<!ELEMENT PATCHABLE (#PCDATA)>

<!ELEMENT VENDOR_REFERENCE_LIST (VENDOR_REFERENCE)+>
<!ELEMENT VENDOR_REFERENCE (ID,URL)>
<!ELEMENT CVE_ID_LIST (CVE_ID)+>
<!ELEMENT CVE_ID (ID,URL)>
<!ELEMENT DIAGNOSIS (#PCDATA)>
<!ELEMENT CONSEQUENCE (#PCDATA)>
<!ELEMENT SOLUTION (#PCDATA)>

<!ELEMENT COMPLIANCE (COMPLIANCE_INFO+)>
<!ELEMENT COMPLIANCE_INFO (COMPLIANCE_TYPE, COMPLIANCE_SECTION,
                           COMPLIANCE_DESCRIPTION)>
<!ELEMENT COMPLIANCE_TYPE (#PCDATA)>
<!ELEMENT COMPLIANCE_SECTION (#PCDATA)>
<!ELEMENT COMPLIANCE_DESCRIPTION (#PCDATA)>

<!ELEMENT CORRELATION (EXPLOITABILITY?,MALWARE?)>
<!ELEMENT EXPLOITABILITY (EXPLT_SRC)+>
<!ELEMENT EXPLT_SRC (SRC_NAME, EXPLT_LIST)>
<!ELEMENT SRC_NAME (#PCDATA)>
<!ELEMENT EXPLT_LIST (EXPLT)+>
<!ELEMENT EXPLT (REF, DESC, LINK?)>
<!ELEMENT REF (#PCDATA)>
<!ELEMENT DESC (#PCDATA)>
<!ELEMENT LINK (#PCDATA)>

<!ELEMENT MALWARE (MW_SRC)+>
<!ELEMENT MW_SRC (SRC_NAME, MW_LIST)>
<!ELEMENT MW_LIST (MW_INFO)+>
<!ELEMENT MW_INFO (MW_ID, MW_TYPE?, MW_PLATFORM?, MW_ALIAS?, MW_RATING?,
                   MW_LINK?)>
<!ELEMENT MW_ID (#PCDATA)>
<!ELEMENT MW_TYPE (#PCDATA)>
<!ELEMENT MW_PLATFORM (#PCDATA)>
<!ELEMENT MW_ALIAS (#PCDATA)>
<!ELEMENT MW_RATING (#PCDATA)>
<!ELEMENT MW_LINK (#PCDATA)>

<!ELEMENT CVSS_BASE (#PCDATA)>
<!ATTLIST CVSS_BASE
    source CDATA #IMPLIED
>
<!ELEMENT CVSS_TEMPORAL (#PCDATA)>
<!ELEMENT CVSS_ACCESS_VECTOR (#PCDATA)>
<!ELEMENT CVSS_ACCESS_COMPLEXITY (#PCDATA)>
```

```
<!ELEMENT CVSS_AUTHENTICATION (#PCDATA)>
<!ELEMENT CVSS_CONFIDENTIALITY_IMPACT (#PCDATA)>
<!ELEMENT CVSS_INTEGRITY_IMPACT (#PCDATA)>
<!ELEMENT CVSS_AVAILABILITY_IMPACT (#PCDATA)>
<!ELEMENT CVSS_EXPLOITABILITY (#PCDATA)>
<!ELEMENT CVSS_REMEDIATION_LEVEL (#PCDATA)>
<!ELEMENT CVSS_REPORT_CONFIDENCE (#PCDATA)>
<!ELEMENT PCI_FLAG (#PCDATA)>

<!ELEMENT PCI_REASONS (PCI_REASON)+>
<!ELEMENT PCI_REASON (#PCDATA)>
```

XPaths for KnowledgeBase Download Output

This section describes the XPaths in the KnowledgeBase download output.

XPath	element specifications / notes
/VULNS	(ERROR | (VULN)+)
/VULNS/VUL N	(QID, VULN_TYPE, SEVERITY_LEVEL, TITLE, CATEGORY?, LAST_UPDATE?, BUGTRAQ_ID_LIST?, PATCHABLE, VENDOR_REFERENCE_LIST?, CVE_ID_LIST?, DIAGNOSIS?, CONSEQUENCE?, SOLUTION?, COMPLIANCE?, CORRELATION?, CVSS_BASE?, CVSS_TEMPORAL?, CVSS_ACCESS_VECTOR?, CVSS_ACCESS_COMPLEXITY?, CVSS_AUTHENTICATION?, CVSS_CONFIDENTIALITY_IMPACT?, CVSS_INTEGRITY_IMPACT?, CVSS_AVAILABILITY_IMPACT?, CVSS_EXPLOITABILITY?, CVSS_REMEDIATION_LEVEL?, CVSS_REPORT_CONFIDENCE?, PCI_FLAG?, PCI_REASONS?)
/VULNS/ERROR	(#PCDATA)
attribute: **number**	**number** is *implied* and, if present, is an error code
/VULNS/VULN/QID	(#PCDATA)
	The Qualys ID (QID) assigned to the vulnerability.
/VULNS/VULN/VULN_TYPE	(#PCDATA)
	The vulnerability type. A valid value is "Vulnerability" for a confirmed vulnerability, "Potential Vulnerability" for a potential vulnerability, "Vulnerability or Potential Vulnerability" for a vulnerability that may be confirmed by the scanning engine during a scan, or "Information Gathered" for information gathered. The type "Vulnerability or Potential Vulnerability" is identified in the Qualys web application with the half red/half yellow icon. If confirmed to exist during a scan, the service reports this as a confirmed vulnerability. If not confirmed, the service reports this as a potential vulnerability. See the Qualys online help for further information.
/VULNS/VULN/SEVERITY_LEVEL	
	(#PCDATA)
	The severity level assigned to the vulnerability. A valid value for a confirmed or potential vulnerability is an integer 1 to 5, where 5 represents the most serious risk if exploited. A valid value for information gathered is a value 1 to 3, where 3 represents the most serious risk if exploited.
/VULNS/VULN/TITLE	(#PCDATA)
	The title of the vulnerability.

Optional Elements

XPath	element specifications / notes
/VULNS/VULN/CATEGORY	(#PCDATA)
	The vulnerability category, from the Qualys KnowledgeBase.
/VULNS/VULN/LAST_UPDATE	(#PCDATA)
	The date this vulnerability was last updated in the Qualys KnowledgeBase, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/VULNS/VULN/BUGTRAQ_ID_LIST	
	(BUGTRAQ_ID+)
/VULNS/VULN/BUGTRAQ_ID_LIST/BUGTRAQ_ID	
	(ID, URL)
	A Bugtraq ID assigned to the vulnerability, and the URL to this Bugtraq ID.
/VULNS/VULN/PATCHABLE	(#PCDATA)
	A flag indicating whether there is a patch available to fix the vulnerability. The value 1 indicates a patch is available to fix the vulnerability. The value 0 indicates a patch is not available to fix the vulnerability.
/VULNS/VULN/VENDOR_REFERENCE_LIST	
	(VENDOR_REFERENCE+)
/VULNS/VULN/VENDOR_REFERENCE_LIST/VENDOR_REFERENCE	
	(ID, URL)
	The name of a vendor reference, and the URL to this vendor reference.
/VULNS/VULN/CVE_ID_LIST	(CVE_ID+)
/VULNS/VULN/CVE_ID_LIST/CVE_ID	(ID, URL)
	A CVE name assigned to the vulnerability, and the URL to this CVE name. CVE (Common Vulnerabilities and Exposures) is a list of common names for publicly known vulnerabilities and exposures. Through open and collaborative discussions, the CVE Editorial Board determines which vulnerabilities or exposures are included in CVE. If the CVE name starts with CAN (candidate) then it is under consideration for entry into CVE.
/VULNS/VULN/DIAGNOSIS	(#PCDATA)
	A description of the threat posed by the vulnerability if successfully exploited.
/VULNS/VULN/CONSEQUENCE	(#PCDATA)
	A description of the consequences that may occur if this vulnerability is successfully exploited.
/VULNS/VULN/SOLUTION	(#PCDATA)
	A verified solution to fix the vulnerability, from the Qualys KnowledgeBase. When virtual patch information is correlated with a vulnerability, the virtual patch information from Trend Micro appears under the heading “Virtual Patches:”. This includes a list of virtual patches and a link to more information.

XPath	element specifications / notes
/VULNS/VULN/COMPLIANCE	(COMPLIANCE_INFO+)
/VULNS/VULN/COMPLIANCE/COMPLIANCE_INFO	(COMPLIANCE_TYPE, COMPLIANCE_SECTION, COMPLIANCE_DESCRIPTION)
/VULNS/VULN/COMPLIANCE/COMPLIANCE_INFO/COMPLIANCE_TYPE	(#PCDATA) The type of a compliance policy or regulation that is associated with the vulnerability. A valid value is: -HIPAA (Health Insurance Portability and Accountability Act) -GLBA (Gramm-Leach-Bliley Act) -CobIT (Control Objectives for Information and related Technology -SOX (Sarbanes-Oxley Act)
/VULNS/VULN/COMPLIANCE/COMPLIANCE_INFO/COMPLIANCE_SECTION	(#PCDATA) The section of a compliance policy or regulation associated with the vulnerability.
/VULNS/VULN/COMPLIANCE/COMPLIANCE_INFO/COMPLIANCE_DESCRIPTION	(#PCDATA) The description of a compliance policy or regulation associated with the vulnerability.
/VULNS/VULN/CORRELATION	(EXPLOITABILITY?, MALWARE?)
/VULNS/VULN/CORRELATION/EXPLOITABILITY	(EXPLT_SRC)+ The <EXPLOITABILITY> element and its sub-elements appear only when there is exploitability information for the vulnerability from third party vendors and/or publicly available sources.
/VULNS/VULN/CORRELATION/EXPLOITABILITY/EXPLT_SRC	(SRC_NAME, EXPLT_LIST)
/VULNS/VULN/CORRELATION/EXPLOITABILITY/EXPLT_SRC/SRC_NAME	(#PCDATA) The name of a third party vendor or publicly available source whose exploitability information is correlated with a certain vulnerability.
/VULNS/VULN/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST	(EXPLT)+
/VULNS/VULN/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT	(REF, DESC, LINK?)
/VULNS/VULN/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/REF	(#PCDATA) The CVE reference for the exploitability information.
/VULNS/VULN/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/DESC	(#PCDATA) The description of the exploitability information provided by the source (third party vendor or publicly available source) for a certain vulnerability.
/VULNS/VULN/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/LINK	(#PCDATA) A link to the exploit for a certain vulnerability, when available from the source.
/VULNS/VULN/CORRELATION/MALWARE	(MW_SRC)+ The <MALWARE> element and its sub-elements appear only when there is malware information for the vulnerability from Trend Micro.
/VULNS/VULN/CORRELATION/MALWARE/MW_SRC	(SRC_NAME, MW_LIST)
/VULNS/VULN/CORRELATION/MALWARE/MW_SRC/SRC_NAME	(#PCDATA) The name of the source of the malware information: Trend Micro.
/VULNS/VULN/CORRELATION/MALWARE/MW_SRC/MW_LIST	(MW_INFO)+

XPath	element specifications / notes
/VULNS/VULN/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO	(MW_ID, MW_TYPE?, MW_PLATFORM?, MW_ALIAS?, MW_RATING?, MW_LINK?)
/VULNS/VULN/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_ID (#PCDATA)	
	The malware name/ID assigned by Trend Micro.
/VULNS/VULN/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_TYPE (#PCDATA)	
	The type of malware, such as Backdoor, Virus, Worm or Trojan.
/VULNS/VULN/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_PLATFORM (#PCDATA)	
	A list of the platforms that may be affected by the malware.
/VULNS/VULN/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_ALIAS (#PCDATA)	
	A list of other names used by different vendors and/or publicly available sources to refer to the same threat.
/VULNS/VULN/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_RATING (#PCDATA)	
	The overall risk rating as determined by Trend Micro: Low, Medium or High.
/VULNS/VULN/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_LINK (#PCDATA)	
	A link to malware details.
/VULNS/VULN/CVSS_BASE	(#PCDATA)
	The CVSS base score assigned to the vulnerability. This value is displayed only when the CVSS scoring feature is enabled in the user account.
attribute: **source**	**source** is *implied* and, if present, is "service" to indicate that the CVSS base score for the vulnerability is not supplied by NIST, as published in the National Vulnerability Database (NVD). The service displays a CVSS base score provided by NIST whenever available. In a case where NIST lists a CVSS base score of 0 or does not provide a score for a vulnerability in the NVD, the service determines whether the severity of the vulnerability warrants a higher CVSS base score. If so, a service generated score is provided and the attribute "source=service" appears in the XML output.
/VULNS/VULN/CVSS_TEMPORAL (#PCDATA)	
	The CVSS temporal score. This value is displayed only when the CVSS scoring feature is enabled in the user account.
/VULNS/VULN/CVSS_ACCESS_VECTOR (#PCDATA)	
	The CVSS access vector metric in the Base Metrics group. This metric reflects how the vulnerability is exploited. The more remote an attacker can be to attack a host, the greater the vulnerability score. The value is one of the following: Network, Adjacent Network, Local Access, or Undefined. This element only appears when the API request includes the parameter **show_cvss_submetrics=1**.
/VULNS/VULN/CVSS_ACCESS_COMPLEXITY (#PCDATA)	
	The CVSS access complexity metric in the Base Metrics group. This metric measures the complexity of the attack required to exploit the vulnerability once an attacker has gained access to the target system. The value is one of the following: Undefined, Low, Medium, or High. This element only appears when the API request includes the parameter **show_cvss_submetrics=1**.

XPath	element specifications / notes
/VULNS/VULN/CVSS_AUTHENTICATION (#PCDATA)	
	The CVSS authentication metric in the Base Metrics group. This metric measures the number of times an attacker must authenticate to a target in order to exploit a vulnerability. The value is: Undefined, Non required, Require single instance, or Require multiple instances. This element only appears when the API request includes the parameter **show_cvss_submetrics=1**.
/VULNS/VULN/CVSS_CONFIDENTIALITY_IMPACT (#PCDATA)	
	The CVSS confidentiality impact metric in the Base Metrics group. This metric measures the impact on confidentiality of a successfully exploited vulnerability. The value is: Undefined, None, Partial, or Complete. This element only appears when the API request includes the parameter **show_cvss_submetrics=1**.
/VULNS/VULN/CVSS_INTEGRITY_IMPACT (#PCDATA)	
	The CVSS integrity impact metric in the Base Metrics group. This metric measures the impact to integrity of a successfully exploited vulnerability. The value is: Undefined, None, Partial, or Complete. This element only appears when the API request includes the parameter **show_cvss_submetrics=1**.
/VULNS/VULN/CVSS_AVAILABILITY_IMPACT (#PCDATA)	
	The CVSS availability impact metric in the Base Metrics group. This metric measures the impact to availability of a successfully exploited vulnerability. The value is: Undefined, None, Partial, or Complete. This element only appears when the API request includes the parameter **show_cvss_submetrics=1**.
/VULNS/VULN/CVSS_EXPLOITABILITY (#PCDATA)	
	The CVSS exploitability metric in the Temporal Metrics group. This metric measures the current state of exploit techniques or code availability. The value is: Undefined, Unproven, Proof-of-concept, Functional, or Widespread. This element only appears when the API request includes the parameter **show_cvss_submetrics=1**.
/VULNS/VULN/CVSS_REMEDIATION_LEVEL (#PCDATA)	
	The CVSS remediation level metric in the Temporal Metrics group. The remediation level of a vulnerability is an important factor for prioritization. The value is: Undefined, Official-fix, Temporary-fix, Workaround, or Unavailable. This element only appears when the API request includes the parameter **show_cvss_submetrics=1**.
/VULNS/VULN/CVSS_REPORT_CONFIDENCE (#PCDATA)	
	The CVSS report confidence metric in the Temporal Metrics group. This metric measures the degree of confidence in the existence of the vulnerability and the credibility of the known technical details. The value is: Undefined, Not confirmed, Uncorroborated, or Confirmed. This element only appears when the API request includes the parameter **show_cvss_submetrics=1**.
/VULNS/VULN/PCI_FLAG (#PCDATA)	
	A flag indicating whether the vulnerability must be fixed to pass PCI compliance. The value 1 indicates the vulnerability must be fixed to pass PCI compliance. The value 0 indicates the vulnerability does not need to be fixed to pass PCI compliance. This element only appears when the API request includes the parameter **show_pci_flag=1**.

XPath	element specifications / notes
/VULNS/VULN/PCI_REASONS	(PCI_REASON)+
/VULNS/VULN/PCI_REASONS/PCI_REASON	(#PCDATA)
	A reason why the vulnerability passed or failed PCI compliance. This element only appears when the CVSS scoring feature is turned on for the user's subscription and the API request includes the parameter **`show_pci_flag=1`**.

APPENDIX B

Map Reports

The **map.php** function returns a map report including an inventory of network devices that were discovered in a domain. Using the **map_report_list.php** function, you can obtain a list of all saved map reports stored on the Qualys server.

This appendix provides details about these reports:

- Map Report — Version 2
- Map Report — Single Domain
- Map Report List

Map Report — Version 2

The network map report Version 2 is an XML report returned from the **map-2.php** function. The map report identifies hosts found during the network discovery, and the discovery methods used to identify services on the hosts found.

The map report — version 2 DTD and XPaths are described below.

DTD for Map Report

The **map-2.php** function returns live map results using the **map-2.dtd** shown below. This is used for live map results only. When you retrieve a saved map report using **map_report.php** function or download a saved map report from the Qualys application, the **map.dtd** is used.

```
<!-- QUALYS MAP-2 DTD -->

<!ELEMENT MAP_REQUEST (MAP*|ERROR*) >

<!-- value is the report ref -->
<!ELEMENT MAP (HEADER?,(IP+|ERROR)?)>

<!ATTLIST MAP
    value CDATA #IMPLIED>

<!ELEMENT ERROR (#PCDATA)*>
<!ATTLIST ERROR number CDATA #IMPLIED>


<!-- INFORMATION ABOUT THE MAP -->
<!ELEMENT HEADER (KEY+, ASSET_GROUPS?, USER_ENTERED_DOMAINS?,
OPTION_PROFILE?)>

<!ELEMENT KEY (#PCDATA)*>
<!ATTLIST KEY
          value CDATA #IMPLIED>

<!ELEMENT ASSET_GROUP (ASSET_GROUP_TITLE)>
<!ELEMENT ASSET_GROUPS (ASSET_GROUP+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>

<!ELEMENT USER_ENTERED_DOMAINS (DOMAIN+, NETBLOCK*)>
<!ELEMENT DOMAIN (#PCDATA)>
<!ELEMENT NETBLOCK (RANGE+)>
<!ELEMENT RANGE (START+, END+)>
<!ELEMENT START (#PCDATA)>
<!ELEMENT END (#PCDATA)>
```

```
<!ELEMENT OPTION_PROFILE (OPTION_PROFILE_TITLE)>
<!ELEMENT OPTION_PROFILE_TITLE (#PCDATA)>
<!ATTLIST OPTION_PROFILE_TITLE
    option_profile_default CDATA #IMPLIED
>

<!-- value is the IP -->
<!-- type is the kind of server : router, mail server ... -->
<!-- "port" is deprecated, replaced by "discovery" -->
<!ELEMENT IP ((PORT*,DISCOVERY*,LINK*)|LINK+)?>
<!ATTLIST IP
    value CDATA #REQUIRED
    name CDATA #IMPLIED
    type CDATA #IMPLIED
    os CDATA #IMPLIED
    netbios CDATA #IMPLIED
    account CDATA #IMPLIED>

<!-- value indicates an open port on a server (deprecated) -->
<!ELEMENT PORT (#PCDATA)*>
<!ATTLIST PORT
    value CDATA #REQUIRED>


<!-- value indicates a method that discovered this machine -->
<!ELEMENT DISCOVERY (#PCDATA)*>
<!ATTLIST DISCOVERY
    method CDATA #REQUIRED>


<!-- value of a link, indicates the need to go trough a server to see -->
<!-- another (ie. gateway or router) -->
<!ELEMENT LINK EMPTY>
<!ATTLIST LINK
    value CDATA #REQUIRED>
```

XPaths for Map Report

This section describes the XPaths in the live map results returned from the **`map-2.php`** function.

XPath	element specification / notes
/MAP	(HEADER?,(IP+ | ERROR)?)
attribute: **`value`**	**`value`** is *implied* and, if present, is the reference number for the map
/MAP/ERROR	(#PCDATA)*
attribute: **`number`**	**`number`** is *implied* and, if present, is an error code
/MAP/HEADER	((KEY+, ASSET_GROUPS?, USER_ENTERED_DOMAINS?, OPTION_PROFILE?)
/MAP/HEADER/KEY	(#PCDATA)*
attribute: **`value`**	**`value`** is *implied* and, if present, will be one of the following: USERNAME..... The Qualys user login name for the user that initiated the map request. COMPANY..... The company associated with the Qualys user. DATE..... The date when the map was started. The date appears in YYYY-MM-DDTHH:MM:SSZ format (in UTC/GMT) like this: "2002-06-08T16:30:15Z" TITLE ..... A descriptive title. TARGET..... The target domain. NBHOST_TOTAL..... The total number of hosts included in the map. DURATION..... The time it took to complete the map. SCAN_HOST ..... The IP address of the host that processed the map. REPORT_TYPE ..... The report type: “API” for an on-demand map request launched from the API, “On-demand” for an on-demand map request launched from the Qualys user interface, and “Scheduled” for a scheduled map. OPTIONS..... The option profile applied to the map. Note that the options information provided may be incomplete. DEFAULT_SCANNER.. The value 1 indicates that the default scanner was enabled for the map. ISCANNER_NAME..... The scanner appliance name or "external" (for external scanner) used for the map. STATUS..... The job status of the map. FINISHED - The scanner(s) have finished the map job, the map results were loaded onto the platform, and hosts were discovered. NOHOSTALIVE - The scanner(s) have finished the map job, the map results were loaded onto the platform, and no devices were discovered. LOADING - The scanner(s) have finished the map job, and the map results are being loaded onto the platform. CANCELED - A user canceled the map, and the scanner(s) have stopped the map job. ERROR - An error occurred during the map, and the map did not complete. INTERRUPTED - The map was interrupted and did not complete.

XPath	element specification / notes
/MAP/HEADER/ASSET_GROUPS (ASSET_GROUP+)	
/MAP/HEADER/ASSET_GROUPS/ASSET_GROUP (ASSET_GROUP_TITLE)	
/MAP/HEADER/ASSET_GROUPS/ASSET_GROUP/ASSET_GROUP_TITLE (#PCDATA)	
	The title of an asset group that was specified as a map target.
/MAP/HEADER/USER_ENTERED_DOMAINS (DOMAIN+, NETBLOCK*)	
/MAP/HEADER/USER_ENTERED_DOMAINS/DOMAIN (#PCDATA)	
	A domain name entered as a target for the map.
/MAP/HEADER/USER_ENTERED_DOMAINS/NETBLOCK (RANGE+)	
/MAP/HEADER/USER_ENTERED_DOMAINS/NETBLOCK/RANGE (START+, END+)	
/MAP/HEADER/USER_ENTERED_DOMAINS/NETBLOCK/RANGE/START (#PCDATA)	
	An IP address that represents the start of the netblock range.
/MAP/HEADER/USER_ENTERED_DOMAINS/NETBLOCK/RANGE/END (#PCDATA)	
	An IP address that represents the end of the netblock range.
/MAP/HEADER/OPTION_PROFILE (OPTION_PROFILE_TITLE)	
/MAP/HEADER/OPTION_PROFILE/OPTION_PROFILE_TITLE (#PCDATA)	
	The title of the option profile, as defined in the Qualys user interface, that was applied to the map.
attribute: **option_profile_default**	**option_profile_default** is *implied* and, if present, is a code that specifies whether the option profile was defined as the default option profile in the user account. A value of 1 is returned when this option profile is the default. A value of 0 is returned when this option profile is not the default.
/MAP/IP	((PORT*,DISCOVERY*,LINK*)|LINK+)?
attribute: **value**	**value** is *required* and is an IP address
attribute: **name**	**name** is *implied* and, if present, is the device's registered DNS host name
attribute: **type**	**type** is *implied* and, if present, will indicate a device type such as "router"
attribute: **os**	**os** is *implied* and, if present, is a string indicating the device's operating system
attribute: **netbios**	**netbios** is *implied* and, if present, is the device's Windows NetBIOS name
attribute: **account**	**account** is *implied* and, if present, will be the following: yes..... The user account allows the IP address to be scanned

XPath	element specification / notes
/MAP/IP/DISCOVERY	(#PCDATA)
attribute: **method**	**method** is *required* and will be one of the following: DNS ..... DNS lookup DNS Zone Transfer..... DNS zone transfer detected ICMP ..... ICMP packets received from the host Reverse_DNS ..... Reverse DNS lookup TCP Port [n] ..... Open TCP port [number] TCP RST..... TCP reset packets received from the host TraceRoute..... Trace route UDP Port [n] ..... Open UDP port [number] Other Protocol or ICMP ..... IP packet received from the host whose protocol is not TCP, UDP, or ICMP Other TCP Ports ..... TCP packet received containing source ports not in the list of probed ports
/MAP/IP/PORT	(#PCDATA)
attribute: **value**	**value** is *required* and will be one of the following: 21 ..... FTP 22 ..... SSH 23 ..... Telnet 25 ..... SMTP 53 ..... DNS 80 ..... HTTP 110..... POP3 139 ..... NetBios 443 ..... HTTPS Note: The PORT element no longer appears in map reports, including new reports and existing reports saved on the Qualys platform. The PORT element may appear in existing reports that you have saved locally.
/MAP/IP/LINK	EMPTY
attribute: **value**	**value** is *required*. If /MAP/IP[@type="router"] then there will be one /MAP/IP/LINK per host found in the domain that is served by that router. In this case, value will be the IP address of the host that this router serves. Otherwise, value is the IP address of the router that serves this host; if value is empty in this case, it means that the router was protected by a firewall or otherwise shielded from discovery.

No Devices Detected

When a network discovery does not detect any devices, live map results are returned. Live map results include header information and an error message. Live map results are not saved on the Qualys server and cannot be retrieved. Sample live map results are shown below.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE MAP_REQUEST SYSTEM "https://qualysapi.qualys.com/map-2.dtd">
<!-- Map is running on: mydomain.com -->
<!-- keep-alive -->
<MAP_REQUEST>
  <MAP value="map/1112217109.26598">
    <HEADER>
      <KEY value="USERNAME">username</KEY>
      <KEY value="COMPANY"><![CDATA[My Company]]></KEY>
      <KEY value="DATE">2005-03-30T21:11:48Z</KEY>
      <KEY value="TITLE"><![CDATA[My Map]]></KEY>
      <KEY value="TARGET">mydomain.com</KEY>
      <KEY value="NBHOST_TOTAL">0</KEY>
      <KEY value="DURATION">00:00:31</KEY>
      <KEY value="SCAN_HOST">hostname (SCANNER 2.9.39-1, WEB 4.0.102-1,
VULNSIGS 1.10.74-1)</KEY>
      <KEY value="REPORT_TYPE">API (default option profile)</KEY>
      <KEY value="STATUS">NOHOSTALIVE</KEY>
      <KEY value="OPTIONS"><![CDATA[Information gathering: All Hosts,
Perform live host sweep, Standard TCP port list, ICMP Host
Discovery]]></KEY>
      <USER_ENTERED_DOMAINS>
        <DOMAIN><![CDATA[mydomain.com]]></DOMAIN>
      </USER_ENTERED_DOMAINS>
      <OPTION_PROFILE>
        <OPTION_PROFILE_TITLE option_profile_default="1"><![CDATA[Initial
Options]]></OPTION_PROFILE_TITLE>
      </OPTION_PROFILE>
    </HEADER>
  </ERROR number="4503">No host found</ERROR>
  </MAP>
  </ERROR number="4503">No host found</ERROR>
</MAP_REQUEST>
```

Map Report — Single Domain

The network map report (map.dtd) is returned from the **map.php** function. The map report identifies hosts found during the network discovery, and the discovery methods used to identify services on the hosts found. When no hosts are found, empty results are returned.

The map report — single domain DTD and XPaths are described below.

DTD for Map Report — Single Domain

A recent DTD for the map report — single domain — returned from the **map.php** function is shown below.

```
<!-- QUALYS MAP DTD -->

<!-- value is the report ref -->
<!ELEMENT MAP (HEADER?,(IP+|ERROR)?) >
<!ATTLIST MAP
    value CDATA #IMPLIED>

<!ELEMENT ERROR (#PCDATA)*>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!-- INFORMATION ABOUT THE MAP -->
<!ELEMENT HEADER (KEY+, ASSET_GROUPS?, USER_ENTERED_DOMAINS?,
OPTION_PROFILE?)>

<!ELEMENT KEY (#PCDATA)*>
<!ATTLIST KEY
          value CDATA #IMPLIED>

<!ELEMENT ASSET_GROUP (ASSET_GROUP_TITLE)>
<!ELEMENT ASSET_GROUPS (ASSET_GROUP+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>

<!ELEMENT USER_ENTERED_DOMAINS (DOMAIN+, NETBLOCK*)>
<!ELEMENT DOMAIN (#PCDATA)>
<!ELEMENT NETBLOCK (RANGE+)>
<!ELEMENT RANGE (START+, END+)>
<!ELEMENT START (#PCDATA)>
<!ELEMENT END (#PCDATA)>

<!ELEMENT OPTION_PROFILE (OPTION_PROFILE_TITLE)>
<!ELEMENT OPTION_PROFILE_TITLE (#PCDATA)>
<!ATTLIST OPTION_PROFILE_TITLE
    option_profile_default CDATA #IMPLIED
>
```

```
<!-- value is the IP -->
<!-- type is the kind of server : router, mail server ... -->
<!-- "port" is deprecated, replaced by "discovery" -->
<!ELEMENT IP ((PORT*,DISCOVERY*,LINK*)|LINK+)?>
<!ATTLIST IP
    value CDATA #REQUIRED
    name CDATA #IMPLIED
    type CDATA #IMPLIED
    os CDATA #IMPLIED
    account CDATA #IMPLIED
    netbios CDATA #IMPLIED>

<!-- value indicates an open port on a server (deprecated) -->
<!ELEMENT PORT (#PCDATA)*>
<!ATTLIST PORT
    value CDATA #REQUIRED>


<!-- value indicates a method that successfully discovered this machine -
->
<!ELEMENT DISCOVERY (#PCDATA)*>
<!ATTLIST DISCOVERY
    method CDATA #REQUIRED>


<!-- value of a link, indicates the need to go trough a server to see -->
<!-- another (ie. gateway or router) -->
<!ELEMENT LINK EMPTY>
<!ATTLIST LINK
    value CDATA #REQUIRED>
```

XPaths for Map Report — Single Domain

This section describes the XPaths in the XML map report — single domain — returned by the **map.php** function.

XPath	element specification / notes
/MAP	(HEADER?,(IP+ | ERROR)?)
attribute: **value**	**value** is *implied* and, if present, is the reference number for the map
/MAP/ERROR	(#PCDATA)*
attribute: **number**	**number** is *implied* and, if present, is an error code
/MAP/HEADER	(KEY)+
/MAP/HEADER/KEY	(PCDATA)*
attribute: **value**	**value** is *implied* and, if present, will be one of the following: USERNAME..... The Qualys user login name for the user that initiated the map request. COMPANY..... The company associated with the Qualys user. DATE..... The date when the map was started. The date appears in YYYY-MM-DDTHH:MM:SSZ format (in UTC/GMT) like this: "2002-06-08T16:30:15Z" TITLE ..... A descriptive title. When the user specifies a title for the map request, the user-supplied title appears. When unspecified, a standard title is assigned. TARGET..... The target domain. NBHOST_TOTAL..... The total number of hosts included in the map. DURATION..... The time it took to complete the map. SCAN_HOST ..... The IP address of the host that processed the map. REPORT_TYPE ..... The report type: “API” for an on-demand map request launched from the API, “On-demand” for an on-demand map request launched from the Qualys user interface, and “Scheduled” for a scheduled map. OPTIONS..... The option profile applied to the map. Note that the options information provided may be incomplete. DEFAULT_SCANNER.. The value 1 indicates that the default scanner was enabled for the map. ISCANNER_NAME..... The name of the scanner appliance applied to the map. STATUS..... The job status of the map. FINISHED - The scanner(s) have finished the map job, the map results were loaded onto the platform, and hosts were discovered. NOHOSTALIVE - The scanner(s) have finished the map job, the map results were loaded onto the platform, and no devices were discovered. LOADING - The scanner(s) have finished the map job, and the map results are being loaded onto the platform. CANCELED - A user canceled the map, and the scanner(s) have stopped the map job. ERROR - An error occurred during the map, and the map did not complete. INTERRUPTED - The map was interrupted and did not complete.

XPath	element specification / notes
/MAP/HEADER/ASSET_GROUPS (ASSET_GROUP+)	
/MAP/HEADER/ASSET_GROUPS/ASSET_GROUP (ASSET_GROUP_TITLE)	
/MAP/HEADER/ASSET_GROUPS/ASSET_GROUP/ASSET_GROUP_TITLE (#PCDATA)	
	The title of an asset group that was specified as a map target.
/MAP/HEADER/USER_ENTERED_DOMAINS (DOMAIN+, NETBLOCK*)	
/MAP/HEADER/USER_ENTERED_DOMAINS/DOMAIN (#PCDATA)	
	A domain name entered as a target for the map.
/MAP/HEADER/USER_ENTERED_DOMAINS/NETBLOCK (RANGE+)	
/MAP/HEADER/USER_ENTERED_DOMAINS/NETBLOCK/RANGE (START+, END+)	
/MAP/HEADER/USER_ENTERED_DOMAINS/NETBLOCK/RANGE/START (#PCDATA)	
	An IP address that represents the start of the netblock range.
/MAP/HEADER/USER_ENTERED_DOMAINS/NETBLOCK/RANGE/END (#PCDATA)	
	An IP address that represents the end of the netblock range.
/MAP/HEADER/OPTION_PROFILE (OPTION_PROFILE_TITLE)	
/MAP/HEADER/OPTION_PROFILE/OPTION_PROFILE_TITLE (#PCDATA)	
	The title of the option profile, as defined in the Qualys user interface, that was applied to the map.
attribute: **option_profile_default**	**option_profile_default** is *implied* and, if present, is a code that specifies whether the option profile was defined as the default option profile in the user account. A value of 1 is returned when this option profile is the default. A value of 0 is returned when this option profile is not the default.
/MAP/IP	(PORT*,DISCOVERY*,LINK*)|LINK+)?
attribute: **value**	**value** is *required* and is an IP address
attribute: **name**	**name** is *implied* and, if present, is an Internet host name
attribute: **type**	**type** is *implied* and, if present, will indicate a device type such as "router"
attribute: **os**	**os** is *implied* and, if present, is a string indicating the device's operating system
attribute: **account**	**account** is *implied* and, if present, will be the following: yes..... The user account allows the IP address to be scanned
attribute: **netbios**	**netbios** is *implied* and, if present, is the device's Windows NetBIOS name

XPath	element specification / notes
/MAP/IP/DISCOVERY	(#PCDATA)
attribute: **method**	**method** is *required* and will be one of the following: DNS ..... DNS lookup DNS Zone Transfer..... DNS zone transfer detected ICMP ..... ICMP packets received from the host Reverse_DNS ..... Reverse DNS lookup TCP Port [n] ..... Open TCP port [number] TCP RST..... TCP reset packets received from the host TraceRoute..... Trace route UDP Port [n] ..... Open UDP port [number] Other Protocol or ICMP ..... IP packet received from the host whose protocol is not TCP, UDP, or ICMP Other TCP Ports ..... TCP packet received containing source ports not in the list of probed ports
/MAP/IP/PORT	(#PCDATA)
attribute: **value**	**value** is *required* and will be one of the following: 21 ..... FTP 22 ..... SSH 23 ..... Telnet 25 ..... SMTP 53 ..... DNS 80 ..... HTTP 110..... POP3 139 ..... NetBios 443 ..... HTTPS Note: The PORT element no longer appears in map reports, including new reports and existing reports saved on the Qualys platform. The PORT element may appear in existing reports that you have saved locally.
/MAP/IP/LINK	EMPTY
attribute: **value**	**value** is *required*. If /MAP/IP[@type="router"] then there will be one /MAP/IP/LINK per host found in the domain that is served by that router. In this case, value will be the IP address of the host that this router serves. Otherwise, value is the IP address of the router that serves this host; if value is empty in this case, it means that the router was protected by a firewall or otherwise shielded from discovery.

Map Report List

The map report list is an XML report returned from the **map_report_list.php** function. All maps for the user account are listed.

The map report list DTD and XPaths are described below.

DTD for Map Report List

A recent DTD for the map report list (map_report_list.dtd) is shown below.

```
<!-- QUALYS MAP_REPORT_LIST DTD -->

<!ELEMENT MAP_REPORT_LIST (ERROR | MAP_REPORT*)>
<!ATTLIST MAP_REPORT_LIST
          user CDATA #REQUIRED
          from CDATA #REQUIRED
          to CDATA #REQUIRED
          with_domain CDATA #IMPLIED>

<!ELEMENT ERROR (#PCDATA)*>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!ELEMENT MAP_REPORT (TITLE, ASSET_GROUPS?, OPTION_PROFILE?)>
<!ATTLIST MAP_REPORT
          ref CDATA #REQUIRED
          date CDATA #REQUIRED
          domain CDATA #REQUIRED
          status CDATA #REQUIRED>

<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT ASSET_GROUP (ASSET_GROUP_TITLE)>
<!ELEMENT ASSET_GROUPS (ASSET_GROUP+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>

<!ELEMENT OPTION_PROFILE (OPTION_PROFILE_TITLE)>
<!ELEMENT OPTION_PROFILE_TITLE (#PCDATA)>
<!ATTLIST OPTION_PROFILE_TITLE
    option_profile_default CDATA #IMPLIED
>
<!-- EOF -->
```

XPaths for Map Report List

This section describes the XPaths in the XML map report list.

XPath	element specification / notes
/MAP_REPORT_LIST	(ERROR | MAP_REPORT*))
attribute: **user**	**user** is *required* and is the Qualys user name.
attribute: **from**	**from** is *required* and is the oldest date in the available map reports, in YYYY-MM-DDTHH:MM:SSZ format (in UTC/GMT) like this: "2002-06-08T16:30:15Z"
attribute: **to**	**to** is *required* and is the newest date in the available map reports, in YYYY-MM-DDTHH:MM:SSZ format (in UTC/GMT)
attribute: **with_domain**	**with_domain** is *implied* and, if present, is a domain found in each of the map reports in the list
/MAP_REPORT_LIST/ERROR	(#PCDATA)*
attribute: **number**	**number** is *implied* and, if present, is an error code
/MAP_REPORT_LIST/MAP_REPORT	(TITLE, ASSET_GROUPS?, OPTION_PROFILE?)
attribute: **ref**	**ref** is *required* and is the reference, or key, for the map
attribute: **date**	**date** is *required* and is the date when the network discovery was performed, in YYYY-MM-DDTHH:MM:SSZ format (in UTC/GMT)
attribute: **domain**	**domain** is *required* and is the domain for which the map was produced
attribute: **status**	**status** is *required* and is the job status reported for the map. QUEUED - A user launched the map or the service started a map based on a map schedule. The map job is waiting to be distributed to scanner(s). RUNNING - The scanner(s) are actively running the map job. LOADING - The scanner(s) finished the map job, and the map results are being loaded onto the platform. FINISHED - The scanner(s) have finished the map job, and the map results were loaded onto the platform. CANCELED - A user canceled the map, the scanner(s) have stopped the map job, and some results may be available. NOHOSTALIVE - The scanner(s) finished the map job, the map results were loaded onto the platform, and target hosts were down (not alive). ERROR - An error occurred during map, and the map did not complete. INTERRUPTED - The map was interrupted and did not complete.
/MAP_REPORT_LIST/MAP_REPORT/TITLE	(#PCDATA)*
	The map title.
/MAP_REPORT_LIST/MAP_REPORT/ASSET_GROUPS	(ASSET_GROUP+)

XPath	element specification / notes
/MAP_REPORT_LIST/MAP_REPORT/ASSET_GROUPS/ASSET_GROUP (ASSET_GROUP_TITLE)	
	(#PCDATA)
	The title of an asset group that was specified as a map target.
/MAP_REPORT_LIST/MAP_REPORT/OPTION_PROFILE (OPTION_PROFILE_TITLE)	
/MAP_REPORT_LIST/MAP_REPORT/OPTION_PROFILE/OPTION_PROFILE_TITLE (#PCDATA)	
	The title of the option profile that was applied to the map.
attribute: **option_profile_default**	**option_profile_default** is *implied* and, if present, specifies whether the option profile was defined as the default in the user account. A valid value is: 1 (option profile is the default), or 0 (option profile is not the default).

APPENDIX C

Preferences Reports

Preferences reports are returned by the preferences functions described in Chapter 4.

This appendix provides details about each of these reports:

- Scheduled Tasks Report
- Scan Options Report
- Scanner Appliance List
- Group List

Scheduled Tasks Report

The scheduled tasks report is an XML report returned from the **scheduled_scans.php** function. This report supports reporting on both scheduled scan and/or map tasks.

The scheduled tasks report DTD and XPaths are described below.

DTD for Scheduled Tasks Report

The DTD for the XML document returned by the **scheduled_scans.php** function, called **scheduled_scans.dtd**, is shown below. It supports reporting on scheduled scans and maps.

```
<!-- QUALYS SCHEDULED TASKS DTD -->

<!ELEMENT SCHEDULEDSCANS (SCAN*|ERROR)>

<!ELEMENT SCAN
(TITLE,TARGETS,SCHEDULE,NEXTLAUNCH_UTC?,DEFAULT_SCANNER?,ISCANNER_NAME?,O
PTION?,TYPE, ASSET_GROUPS?, EXCLUDE_IP_PER_SCAN?, USER_ENTERED_DOMAINS?,
USER_ENTERED_IPS?, NETWORK_ID?,OPTION_PROFILE?)>
<!ATTLIST SCAN
    active (yes|no) #REQUIRED
    ref CDATA #REQUIRED>

<!ELEMENT TITLE (#PCDATA)>
<!-- Option profile -->
<!ELEMENT OPTION (#PCDATA)>
<!-- Type: SCAN or MAP -->
<!ELEMENT TYPE (#PCDATA)>

<!ELEMENT TARGETS (#PCDATA)>

<!--
Schedule is daily or weekly or monthly.
Start_Date is CCYY-MM-DD-Thh:mm:ss
end_after implies number of hours after which scan
should be terminated if not finished.
Recurrence is max count the schedule will be executed.
-->
<!ELEMENT SCHEDULE
((DAILY|WEEKLY|MONTHLY|RELAUNCH_ON_FINISH),START_DATE_UTC,START_HOUR,STAR
T_MINUTE,END_AFTER_HOURS?,PAUSE_AFTER_HOURS?,RESUME_IN_DAYS?,TIME_ZONE,DS
T_SELECTED,RECURRENCE?)>

<!ELEMENT RELAUNCH_ON_FINISH EMPTY>
<!ELEMENT DAILY EMPTY>
<!ATTLIST DAILY
```

```
        frequency_days  CDATA #REQUIRED>

<!-- weekdays is comma-separated list of weekdays e.g. 0,1,4,5 -->
<!ELEMENT WEEKLY EMPTY>
<!ATTLIST WEEKLY
        frequency_weeks  CDATA #REQUIRED
        weekdays   CDATA #REQUIRED>

<!-- either day of month, or (day of week and week of month) must be
provided -->
<!ELEMENT MONTHLY EMPTY>
<!ATTLIST MONTHLY
        frequency_months  CDATA #REQUIRED
        day_of_month  CDATA  #IMPLIED
        day_of_week  (0|1|2|3|4|5|6)  #IMPLIED
        week_of_month  (1|2|3|4|5)  #IMPLIED>

<!-- start date of the task in UTC -->
<!ELEMENT START_DATE_UTC (#PCDATA)>
<!-- User Selected hour -->
<!ELEMENT START_HOUR (#PCDATA)>
<!-- User Selected Minute -->
<!ELEMENT START_MINUTE (#PCDATA)>
<!-- end after how many hours -->
<!ELEMENT END_AFTER_HOURS (#PCDATA)>
<!-- pause after how many hours -->
<!ELEMENT PAUSE_AFTER_HOURS (#PCDATA)>
<!-- if paused then resume after how many days -->
<!ELEMENT RESUME_IN_DAYS (#PCDATA)>
<!ELEMENT TIME_ZONE (TIME_ZONE_CODE,TIME_ZONE_DETAILS)>

<!-- timezone code like US-CA -->
<!ELEMENT TIME_ZONE_CODE (#PCDATA)>

<!-- timezone details like (GMT-0800) United States (California): Los
Angeles, Sacramento, San Diego, San Francisco-->
<!ELEMENT TIME_ZONE_DETAILS (#PCDATA)>

<!-- Did user select DST? 0-not selected 1-selected -->
<!ELEMENT DST_SELECTED (#PCDATA)>
<!ELEMENT RECURRENCE EMPTY>
<!ATTLIST RECURRENCE
        value CDATA #REQUIRED>


<!--
NEXTLAUNCH_UTC is in CCYY-MM-DD-Thh:mm:ss see:
http://www.w3.org/TR/xmlschema-2/#dateTime
-->
```

```
<!ELEMENT NEXTLAUNCH_UTC (#PCDATA)>
<!ELEMENT DEFAULT_SCANNER (#PCDATA)>
<!ELEMENT ISCANNER_NAME (#PCDATA)>

<!ELEMENT ERROR (FIELD*,SUMMARY)>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!ELEMENT FIELD (#PCDATA)*>
<!ATTLIST FIELD
          name
(add_task|drop_task|scan_title|type|active|scan_target|option|occurrence|
time_zone|start_hour|start_date|start_minute|iscanner_name|frequency_days
|frequency_weeks|frequency_months|weekdays|day_of_week|day_of_month|week_
of_month|end_after|recurrence|observe_dst|exclude_ip_per_scan) #REQUIRED
          error_type (invalid|missing) #REQUIRED>

<!ELEMENT SUMMARY (#PCDATA)>

<!-- NAME of the asset group with the TYPE attribute with possible values
of (DEFAULT | EXTERNAL | ISCANNER) -->
<!ELEMENT ASSET_GROUP (ASSET_GROUP_TITLE, NETWORK_ID?)>
<!ELEMENT ASSET_GROUPS (ASSET_GROUP+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>

<!ELEMENT EXCLUDE_IP_PER_SCAN (#PCDATA)>
<!ATTLIST EXCLUDE_IP_PER_SCAN
network_id  CDATA  #IMPLIED
>
<!ELEMENT USER_ENTERED_DOMAINS (DOMAIN*)>
<!ELEMENT DOMAIN (DOMAIN_NAME+, NETBLOCK*)>
<!ELEMENT DOMAIN_NAME (#PCDATA)>
<!ATTLIST DOMAIN_NAME
network_id  CDATA  #IMPLIED
>
<!ELEMENT NETBLOCK (RANGE+)>
<!ELEMENT RANGE (START+, END+)>
<!ELEMENT START (#PCDATA)>
<!ELEMENT END (#PCDATA)>

<!ELEMENT USER_ENTERED_IPS (RANGE*)>
<!ATTLIST USER_ENTERED_IPS
network_id  CDATA  #IMPLIED
>
<!ELEMENT OPTION_PROFILE (OPTION_PROFILE_TITLE)>
<!ELEMENT OPTION_PROFILE_TITLE (#PCDATA)>
<!ATTLIST OPTION_PROFILE_TITLE
    option_profile_default CDATA #IMPLIED
>
```

XPaths for Scheduled Tasks Report

This section describes the XPaths for the scheduled tasks report. Scheduled scans and/or maps may be included.

XPath	element specifications / notes
/SCHEDULEDSCANS	(SCAN* | ERROR)
/SCHEDULEDSCANS/SCAN	(TITLE,TARGETS,SCHEDULE,NEXTLAUNCH_UTC?,DEFAULT_SCANNER?, ISCANNER_NAME?,OPTION?,TYPE, ASSET_GROUPS?, EXCLUDE_IP_PER_SCAN?, USER_ENTERED_DOMAINS?, USER_ENTERED_IPS?, NETWORK_ID?, OPTION_PROFILE?)
attribute: **active**	**active** is *required* and indicates whether the scheduled task is active
attribute: **ref**	**ref** is *required* and is the task ID for the scheduled task
/SCHEDULEDSCANS/SCAN/TITLE (#PCDATA)	
	The title of the scheduled task.
/SCHEDULEDSCANS/SCAN/TARGETS (#PCDATA)	
	The target of the scheduled task -- IPs, domains, and/or asset groups
/SCHEDULEDSCANS/SCAN/SCHEDULE	
	(DAILY|WEEKLY|MONTHLY|LAUNCH_ON_FINISH), START_DATE_UTC, START_HOUR, START_MINUTE, END_AFTER_HOURS?, PAUSE_AFTER_HOURS?, RESUME_IN_DAYS?, TIME_ZONE, DST_SELECTED, RECURRENCE?)
/SCHEDULEDSCANS/SCAN/SCHEDULE/DAILY	
attribute: **frequency_days**	**frequency_days** is *required* and indicates the frequency with which the task will run, expressed as a number of days (from 1 to 365)
/SCHEDULEDSCANS/SCAN/SCHEDULE/WEEKLY	
attribute: **frequency_weeks**	**frequency_weeks** is *required* and indicates the frequency with which the weekly task is defined to run, expressed as a number of weeks (from 1 to 52)
attribute: **weekdays**	**weekdays** is *required* an indicates on which weekdays the weekly task is defined to run (from 0 to 6), where 0 is Sunday and 6 is Saturday and multiple weekdays are comma separated
/SCHEDULEDSCANS/SCAN/SCHEDULE/MONTHLY	
attribute: **frequency_months**	**frequency_months** is *required* and indicates the frequency with which the monthly task will run, expressed as a number of months (from 1 to 12)
attribute: **day_of_month**	**day_of_month** is *implied* and, if present, indicates the day of month to run the monthly task, when the task runs on the Nth day of the month (from 0 to 31)
attribute: **day_of_week**	**day_of_week** is *implied* and, if present, indicates the day of week to run the monthly task, when the task runs on a weekday on the Nth day of the month (from 0 to 6), where 0 is Sunday and 6 is Saturday
attribute: **week_of_month**	**week_of_month** is *implied* and, if present, indicates the Nth week of the month to run the monthly task when the task runs on a weekday on the Nth day of the month (from 1 to 5), where 1 is the first week of the month and 5 is the fifth week of the month

XPath	element specifications / notes
/SCHEDULEDSCANS/SCAN/SCHEDULE/RELAUNCH_ON_FINISH	
	This element appears when the task is configured with the "Relaunch on Finish" option. When configured, the service launches a new scan as soon as the previous one finishes. This gives users the ability to perform continuous scanning.
/SCHEDULEDSCANS/SCAN/SCHEDULE/START_DATE_UTC (#PCDATA)	
	The start date defined for the task in UTC format.
/SCHEDULEDSCANS/SCAN/SCHEDULE/START_HOUR (#PCDATA)	
	The start hour defined for the task.
/SCHEDULEDSCANS/SCAN/SCHEDULE/START_MINUTE (#PCDATA)	
	The start minute defined for the task.
/SCHEDULEDSCANS/SCAN/SCHEDULE/END_AFTER_HOURS (#PCDATA)	
	The number of hours to wait for the task to complete before it is deactivated.
/SCHEDULEDSCANS/SCAN/SCHEDULE/PAUSE_AFTER_HOURS (#PCDATA)	
	The "pause after number of hours" run time setting defined for the task.
/SCHEDULEDSCANS/SCAN/SCHEDULE/RESUME_IN_DAYS (#PCDATA)	
	The "resume in number of days" setting defined for the task.
/SCHEDULEDSCANS/SCAN/SCHEDULE/TIME_ZONE	
	(TIME_ZONE_CODE,TIME_ZONE_DETAILS)
/SCHEDULEDSCANS/SCAN/SCHEDULE/TIME_ZONE/TIME_ZONE_CODE (#PCDATA)	
	The time zone code defined for the task. For example: US-CA. If a GMT shift value was specified to add the task in the time_zone parameter of scheduled_scans.php, the GMT shift value is translated automatically to an equivalent time zone code and reported in this element. For more information, see "Automatic Translation — GMT Shift to Time Zone Code" below.
/SCHEDULEDSCANS/SCAN/SCHEDULE/TIME_ZONE/TIME_ZONE_DETAILS (#PCDATA)	
	The time zone details (description) for the local time zone, identified in the <TIME_ZONE_CODE> element. For example:, (GMT-0800) United States (California): Los Angeles, Sacramento, San Diego, San Francisco.
/SCHEDULEDSCANS/SCAN/SCHEDULE/DST_SELECTED	
	When set to 1, Daylight Saving Time (DST) is enabled for the task.
/SCHEDULEDSCANS/SCAN/SCHEDULE/RECURRENCE	
attribute: **value**	**value** is *required* and indicates the number of times the task will be run before it is deactivated (from 1 to 99)
/SCHEDULEDSCANS/SCAN/NEXTLAUNCH_UTC (#PCDATA)	
	The next date and time when the task will be launched.
/SCHEDULEDSCANS/SCAN/DEFAULT_SCANNER (#PCDATA)	
	A value (0 or 1) indicating whether the default scanner is enabled for the task. 1 is returned when the default scanner is enabled for the task, and 0 is returned when the default scanner is disabled for the task. This element is included in the report only when one or more scanner appliances are in the user account.

XPath	element specifications / notes
/SCHEDULEDSCANS/SCAN/ISCANNER_NAME (#PCDATA)	
	The scanner appliance assigned to the task.The value returned can be a scanner appliance name, "default" for the default scanner, or "external" for the external scanners. This element is included in the report only when one or more scanner appliances are in the user account.
/SCHEDULEDSCANS/SCAN/OPTION (#PCDATA)	
	The option profile name assigned to the task.
/SCHEDULEDSCANS/SCAN/TYPE (#PCDATA)	
	The task type, either "scan" or "map".
/SCHEDULEDSCANS/SCAN/ERROR	
	(FIELD*,SUMMARY)
attribute: **number**	**number** is *implied* and, if present, is an error code
/SCHEDULEDSCANS/SCAN/ERROR/FIELD (#PCDATA)	
attribute: **name**	**name** is *required* and indicates information about the scheduled task (scan or map); values correspond to "scheduled_scans.php" input parameters
attribute: **error_type**	**error_type** is *required* and indicates whether the field is invalid or missing: invalid ..... The attribute value is invalid missing..... The attribute value is missing
/SCHEDULEDSCANS/SCAN/ERROR/SUMMARY (#PCDATA)	
	The error summary.
/SCHEDULED_SCANS/SCAN/ASSET_GROUPS (ASSET_GROUP+)	
/SCHEDULED_SCANS/SCAN/ASSET_GROUPS/ASSET_GROUP (ASSET_GROUP_TITLE, NETWORK_ID?)	
/SCHEDULED_SCANS/SCAN/ASSET_GROUPS/ASSET_GROUP/ASSET_GROUP_TITLE (#PCDATA)	
	The title of an asset group that is included in the task target.
/SCHEDULED_SCANS/SCAN/ASSET_GROUPS/ASSET_GROUP/NETWORK_ID (#PCDATA)	
	The network ID assigned to the asset group (appears only when the user has access to custom networks).
/SCHEDULEDSCANS/SCAN/EXCLUDE_IP_PER_SCAN (#PCDATA)	
	The IP addresses/ranges that are excluded for the scheduled scan.
attribute: **network_id**	**network_id** is *implied* and, if present, is the network ID associated with the IPs/ranges excluded from the scan target (appears only when the user has access to custom networks)
/SCHEDULEDSCANS/SCAN/USER_ENTERED_DOMAINS (DOMAIN*)	
/SCHEDULEDSCANS/SCAN/USER_ENTERED_DOMAINS/DOMAIN (DOMAIN_NAME+, NETBLOCK*)	
/SCHEDULEDSCANS/SCAN/USER_ENTERED_DOMAINS/DOMAIN/DOMAIN_NAME (#PCDATA)	
	The domain name defined for the scheduled map target.
attribute: **network_id**	**network_id** is *implied* and, if present, is the network ID associated with the domain name (appears only when the user has access to custom networks)
/SCHEDULEDSCANS/SCAN/USER_ENTERED_DOMAINS/DOMAIN/NETBLOCK (#PCDATA)	
	The netblock associated with a domain asset.

XPath	element specifications / notes
/SCHEDULEDSCANS/SCAN/USER_ENTERED_DOMAINS/DOMAIN/RANGE (START+, END+)	
/SCHEDULEDSCANS/SCAN/USER_ENTERED_DOMAINS/DOMAIN/DOMAIN_NAME/RANGE/START (#PCDATA)	
	The starting IP address of an IP address range.
/SCHEDULEDSCANS/SCAN/USER_ENTERED_DOMAINS/DOMAIN/DOMAIN_NAME/RANGE/START (#PCDATA)	
	The ending IP address of an IP address range.
/SCHEDULEDSCANS/SCAN/USER_ENTERED_IPS (RANGE*)	
	The IP addresses/ranges defined for the scheduled scan target by the user.
attribute: **network_id**	**network_id** is *implied* and, if present, is the network ID associated with the IPs/ranges (appears only when the user has access to custom networks)
/SCHEDULED_SCANS/SCAN/OPTION_PROFILE (OPTION_PROFILE_TITLE)	
/SCHEDULED_SCANS/SCAN/OPTION_PROFILE/OPTION_PROFILE_TITLE (#PCDATA)	
	The title of the option profile, as defined in the Qualys user interface, that is applied to the task.
attribute: **option_profile_default**	**option_profile_default** is *implied* and, if present, is a value (0 or 1) that indicates whether the option profile is defined as the default option profile in the user account. 1 is returned when the option profile is the default, 0 is returned when the option profile is not the default.

Automatic Translation — GMT Shift to Time Zone Code

To add a scheduled task using the **scheduled_scans.php** function, you must specify the local time zone for the task. You have the option to specify a time zone code using the **time_zone_code** parameter or a GMT shift using the **time_zone** parameter. For further information, see "Time Zone Selection" in Chapter 4.

When the **time_zone** parameter with GMT shift is used, the **scheduled_scans.php** function automatically translates the GMT shift to an equivalent time zone code. This time zone code is included the scheduled scans report returned from **scheduled_scans.php** in the <TIME_ZONE_CODE> element. The time zone code also appears when viewing/editing a scheduled task in the Qualys user interface.

The translation to the time zone code ensures that your scheduled tasks run at the local time. The translation of the various GMT shift values is provided below, where "code" represents the value returned in the <TIME_ZONE_CODE> element and "details" represents the value returned in the <TIME_ZONE_DETAILS> element.

GMT shift	code	details
-11	AS	American Samoa: Pago Pago
-10	US-HI	United States (Hawaii): Honolulu
-9	US-AK	United States (Alaska): Anchorage, Juneau, Nome
-8	US-CA	United States (California): Los Angeles, Sacramento, San Diego, San Francisco
-7	US-AZ	United States (Arizona): Phoenix. Tuscon
-6	US-TX	United States (Texas): Austin, Dallas, Houston, San Antonio
-5	US-NY	United States (New York): New York, Albany, Buffalo
-4	PR	Puerto Rico: San Juan
-3	BR-RJ	Brazil (Rio de Janeiro): Rio de Janeiro
-2	BR-FN	Brazil (Fernando de Noronha)
-1	CV	Cape Verde: Praia
0	GB	United Kingdom: London, Belfast, Birmingham, Cardiff, Edinburgh, Glasgow
+1	FR	France: Paris
+2	GR	Greece: Athens
+3	RU-MOW	Russia (Moscow City)
+4	AE	United Arab Emirates: Abu Dhabi, Dubai
+5	PK	Pakistan: Islamabad, Karachi
+6	LK	Sri Lanka, Colombo
+7	TH	Thailand, Bangkok
+8	CN	China: Beijing, Chengdu, Chongqing, Shanghai, Wuhan
+9	JP	Japan: Kyoto, Osaka, Tokyo, Yokohama
+10	AU-NSW	Austalia (New South Wales): Sydney
+11	NC	New Caledonia
+12	NZ	New Zealand: Auckland, Wellington

DTD for Time Zone Code List

The DTD for the XML document returned by the **time_zone_code_list.php** function, called **time_zone_code_list.dtd**, is shown below.

```
<!-- QUALYS TIME ZONE CODES DTD -->

<!ELEMENT TIME_ZONES (TIME_ZONE*)>
```

```
<!ELEMENT TIME_ZONE (TIME_ZONE_CODE,TIME_ZONE_DETAILS,DST_SUPPORTED)>

<!-- Code to be used in schedule scan api US-CA -->
<!ELEMENT TIME_ZONE_CODE (#PCDATA)>
<!-- details like GMT+0100 country and citylist -->
<!ELEMENT TIME_ZONE_DETAILS (#PCDATA)>
<!-- does this timezone support dst -->
<!ELEMENT DST_SUPPORTED (#PCDATA)>
<!-- EOF -->
```

Each <TIME_ZONE> element identifies a time zone properties, including the code, in the sub-elements described below.

Element	Description
<TIME_ZONE_CODE>	A time zone code. These are pre-defined codes.
<TIME_ZONE_DETAILS>	Text describing the time zone.
<DST_SUPPORTED>	A value (0 or 1) indicating whether the time zone supports Daylight Saving Time (DST). 1 is reported when DST is supported, and 0 is reported when DST is not supported.

Scan Options Report

The scan options report includes information about options set in the default option profile of the API user account. The scan options report is an XML report returned from the **scan_options.php** function. All scan options settings for the user account are included.

The scan options report DTD and XPaths are described below.

DTD for Scan Options Report

A recent DTD for the scan options report is shown below.

```
<!-- QUALYS SCAN OPTIONS DTD -->

<!ELEMENT SCANNEROPTIONS ((SCANDEADHOSTS,PORTS,LOADBALANCER)|ERROR)>
<!ELEMENT SCANDEADHOSTS EMPTY>
<!ATTLIST SCANDEADHOSTS
      value (yes|no) #REQUIRED>
<!ELEMENT PORTS (#PCDATA)>
<!-- element value is the range if @portrange="custom" -->
<!ATTLIST PORTS
     range (default|full|custom|additional|light|none) #REQUIRED>

<!ELEMENT LOADBALANCER EMPTY>
<!ATTLIST LOADBALANCER
     value (yes|no) #REQUIRED>
<!-- ((#PCDATA) | (FIELD+, SUMMARY)) does not work, so we use ANY -->
<!ELEMENT ERROR ANY>
<!ATTLIST ERROR
     number CDATA #IMPLIED>
<!ELEMENT FIELD (#PCDATA)>
<!ATTLIST FIELD
    name (scandeadhosts|portsrange|customrange|maxbandwidth|loadbalancer)
#REQUIRED
     error_type (invalid|missing) #REQUIRED>
<!ELEMENT SUMMARY (#PCDATA)>
<!-- EOF -->
```

XPaths for Scan Options Report

This section describes the XPaths in the XML scan options report.

XPath	element specifications / notes
/SCANNEROPTIONS	((SCANDEADHOSTS,PORTS,LOADBALANCER) | ERROR)
/SCANNEROPTIONS/SCANDEADHOSTS	
attribute: **value**	**value** is *required* and is one of the following: yes ..... The service is invalid no ..... The service does not scan dead hosts
/SCANNEROPTIONS/PORTS	(#PCDATA)*
attribute: **range**	**range** is *required* and will be one of the following: default ..... Standard scan using the Standard TCP ports list (commonly-used ports) full ..... Full scan of all TCP ports custom ..... Custom scan using user-defined TCP ports list additional ..... Standard scan using Standard TCP ports list plus additional, user-defined ports list light ..... Light scan using the Light TCP ports list; also may indicate light scan using the Light TCP ports list plus additional, user-defined ports list none ..... None of the TCP ports scanned
/SCANNEROPTIONS/LOADBALANCER	
attribute: **value**	**value** is *required* and is one of the following: yes ..... The service checks for load balanced hosts; when found, all systems behind load balanced hosts are scanned no ..... The service does not check for load balanced hosts
/SCANNEROPTIONS/ERROR	
attribute: **number**	**number** is *implied* and, if present, is an error code
/SCANNEROPTIONS/ERROR/FIELD	
attribute: **name**	**name** is *required* and is one of the following: scandeadhosts ..... Error with scan dead hosts setting portstoscan ..... Error with scan port range setting customrange ..... Error with scan custom range setting loadbalancer ..... Error with scan load balanced hosts setting
attribute: **error_type**	**error_type** is *required* and is one of the following: invalid ..... The field value is invalid missing ..... A required field is missing
/SCANNEROPTIONS/ERROR/SUMMARY	

Scanner Appliance List

The Scanner Appliance list is an XML report is returned from the **iscanner_list.php** function. This report includes information about the Scanner Appliances that are assigned to the Qualys account.

The Scanner Appliance list DTD and XPaths are described below.

DTD for Scanner Appliance List

A recent DTD for the Scanner Appliance list is shown below.

```
<!-- QUALYS SCANNER APPLIANCE LIST DTD -->

<!ELEMENT ISCANNER_LIST (ISCANNER*|ERROR)>

<!ELEMENT ISCANNER (NAC_ENABLED?, NAM_ENABLED?)>
<!ATTLIST ISCANNER
          id CDATA #REQUIRED
          name CDATA #REQUIRED
          ip CDATA #REQUIRED
          interval CDATA #REQUIRED
          status CDATA #REQUIRED>
<!ELEMENT NAC_ENABLED (#PCDATA)>
<!ELEMENT NAM_ENABLED (#PCDATA)>
<!ELEMENT ERROR (#PCDATA)*>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!-- EOF -->
```

XPaths for Scanner Appliance List

This section describes the XPaths for the Scanner Appliance list.

XPath	element specifications / notes
/ISCANNER_LIST	(ISCANNER*|ERROR)
/ISCANNER_LIST/ISCANNER	(NAC_ENABLED?, NAM_ENABLED?)
attribute: **id**	**id** is *required* and is the Qualys ID assigned to the Scanner Appliance.
attribute: **name**	**name** is *required* and is the name of the Scanner Appliance.
attribute: **ip**	**ip** is *required* and is the IP address assigned to the Scanner Appliance.
attribute: **interval**	**interval** is *required* and is the polling interval, in seconds, assigned to the Scanner Appliance.

XPath	element specifications / notes
attribute: **status**	**status** is *required* and is the status of the scanner appliance. The status "online" indicates the scanner appliance responded to the latest heartbeat check and contacted the Qualys Security Operations Center at that time. The status "offline" indicates the scanner appliance did not respond to the latest heartbeat check and did not contact the Qualys Security Operations Center at that time. The service automatically performs a heartbeat check every 4 hours.
/ISCANNER_LIST/ISCANNER\NAC_ENABLED (#PCDATA)	
	A value (0 or 1) indicating whether the scanner appliance is enabled for Cisco NAC. 1 is returned when NAC is enabled for the appliance, and 0 is returned when NAC is not enabled for the appliance. This element is included in the report only when the NAC feature is enabled in the user account (subscription level feature that can be enabled by Qualys).
/ISCANNER_LIST/ISCANNER\NAM_ENABLED (#PCDATA)	
	A value (0 or 1) indicating whether the scanner appliance is enabled for Qualys NAM. 1 is returned when NAM is enabled for the appliance, and 0 is returned when NAM is not enabled for the appliance. This element is included in the report only when the NAM feature is enabled in the user account (subscription level feature that can be enabled by Qualys).
/ISCANNER_LIST/ERROR	(#PCDATA)*
attribute: **error**	**error** is *implied* and, if present, is an error code.

Group List

The group list is an XML report is returned from the **group_list.php** function. This report includes information about the asset groups defined in the user account.

The group list DTD is described below.

DTD for Group List

A recent DTD for the group list (group_list.dtd) is shown below.

```
<!-- QUALYS ASSET GROUP LIST DTD -->

<!ELEMENT GROUP_LIST (GROUP*)>
<!ELEMENT GROUP (NAME, SCANIPS?, MAPDOMAINS?, SCANNER_APPLIANCES?,
COMMENTS?)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT SCANIPS (IP+)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT MAPDOMAINS (DOMAIN+)>
<!ELEMENT DOMAIN (#PCDATA)>
<!ATTLIST DOMAIN
        netblock CDATA #IMPLIED
>
<!ELEMENT SCANNER_APPLIANCE
(SCANNER_APPLIANCE_NAME,SCANNER_APPLIANCE_SN+)>
<!ELEMENT SCANNER_APPLIANCES (SCANNER_APPLIANCE*)>
<!ELEMENT SCANNER_APPLIANCE_NAME (#PCDATA)>
<!ELEMENT SCANNER_APPLIANCE_SN (#PCDATA)>
<!ATTLIST SCANNER_APPLIANCE
        asset_group_default CDATA #IMPLIED
>
<!ELEMENT COMMENTS (#PCDATA)>
<!-- EOF -->
```

XPaths for Group List

This section describes the XPaths for the group list (group_list.dtd).

XPath	element specifications / notes
/GROUP_LIST	(GROUP*)
/GROUP_LIST/GROUP	(NAME, SCANIPS?, MAPDOMAINS?, SCANNER_APPLIANCES?, COMMENTS?)
/GROUP_LIST/NAME	(#PCDATA)
/GROUP_LIST/SCANIPS	(IP+)
/GROUP_LIST/IP	(#PCDATA)
/GROUP_LIST/MAPDOMAINS	(DOMAIN+)
/GROUP_LIST/DOMAIN	(#PCDATA)
attribute: **netblock**	**netblock** is *implied* and, if present, is netblock information associated with the domain.
/GROUP_LIST/COMMENTS	(#PCDATA)
/GROUP_LIST/SCANNER_APPLIANCES	(SCANNER_APPLIANCE*)
/GROUP_LIST/SCANNER_APPLIANCES/SCANNER_APPLIANCE	(SCANNER_APPLIANCE_NAME,SCANNER_APPLIANCE_SN+)
attribute: **asset_group_default**	**asset_group_default** is *implied* and, if present, indicates whether the scanner appliance is the default scanner in the asset group.
/GROUP_LIST/SCANNER_APPLIANCES/SCANNER_APPLIANCE/SCANNER_APPLIANCE_NAME	(#PCDATA)
	The name of the scanner appliance.
/GROUP_LIST/SCANNER_APPLIANCES/SCANNER_APPLIANCE/SCANNER_APPLIANCE_SN	(#PCDATA)
	The serial number of the scanner appliance.

APPENDIX D

Asset Management Reports

The XML reports returned by the asset management functions are described in this appendix. These reports are covered:

- Asset IP List
- Asset Domain List
- Asset Group List
- Asset Search Report
- Asset Range Info Report
- Asset Data Report

Asset IP List

The asset IP list is an XML report that is returned from the **asset_ip_list.php** function and the **ip_list.php** function. This report includes information about the IP addresses in the subscription.

The asset IP list DTD and XPaths are described below.

DTD for Asset IP List

A recent DTD for the asset IP list (ip_list.dtd) is shown below.

```
<!-- QUALYS IP LIST DTD -->

<!ELEMENT HOST_LIST (ERROR | (IP_LIST, RESULTS?, NO_RESULTS?))>

<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!ELEMENT IP_LIST (RANGE*)>

<!ELEMENT RANGE (START, END)>
<!ELEMENT START (#PCDATA)>
<!ELEMENT END (#PCDATA)>

<!ELEMENT RESULTS (HOST+)>

<!ELEMENT HOST (ERROR | (IP, TRACKING_METHOD, DNS?, NETBIOS?,
                         OPERATING_SYSTEM?, OWNER?, COMMENT?,
                         USER_DEFINED_ATTR_LIST?))>

<!ELEMENT TRACKING_METHOD (VALUE, IP_LIST*)>
<!ELEMENT VALUE (#PCDATA)>

<!ELEMENT IP (#PCDATA)>

<!ELEMENT DNS (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT OPERATING_SYSTEM (#PCDATA)>

<!ELEMENT COMMENT (VALUE, IP_LIST*)>

<!ELEMENT OWNER (FIRSTNAME, LASTNAME, USER_LOGIN, IP_LIST*)>
<!ELEMENT FIRSTNAME (#PCDATA)>
<!ELEMENT LASTNAME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
```

```
<!ELEMENT USER_DEFINED_ATTR_LIST (USER_DEFINED_ATTR+)>
<!ELEMENT USER_DEFINED_ATTR (UDA_INDEX, UDA_TITLE, UDA_VALUE, IP_LIST*)>
<!ELEMENT UDA_INDEX (#PCDATA)>
<!ELEMENT UDA_TITLE (#PCDATA)>
<!ELEMENT UDA_VALUE (#PCDATA)>

<!ELEMENT NO_RESULTS (ERROR | (COMMENT_LIST?, OWNER_LIST?,
                               USER_DEFINED_ATTR_LIST?,
                               TRACKING_METHOD_LIST?))>

<!ELEMENT COMMENT_LIST (COMMENT+)>
<!ELEMENT OWNER_LIST (OWNER+)>
<!ELEMENT TRACKING_METHOD_LIST (TRACKING_METHOD+)>
```

XPaths for Asset IP List

This section describes the XPaths for the asset IP list (ip_list.dtd).

XPath	element specifications / notes
/HOST_LIST	(ERROR | (IP_LIST, RESULTS?, NO_RESULTS?))
/HOST_LIST/ERROR	(#PCDATA)
attribute: **number**	**number** is *implied* and if present, will be an error code.
/HOST_LIST/IP_LIST	(RANGE*)
/HOST_LIST/IP_LIST/RANGE	(START, END)
/HOST_LIST/IP_LIST/RANGE/START	(#PCDATA)
	An IP address that represents the start of an IP range.
/HOST_LIST/IP_LIST/RANGE/END	(#PCDATA)
	An IP address that represents the end an IP range.
/HOST_LIST/RESULTS	(HOST+)
/HOST_LIST/RESULTS/HOST	(ERROR | (IP, TRACKING_METHOD, DNS?, NETBIOS?, OPERATING_SYSTEM?, OWNER?, COMMENT?, USER_DEFINED_ATTR_LIST?))
/HOST_LIST/RESULTS/HOST/IP	(#PCDATA)
	The IP address of the host for which details are reported.
/HOST_LIST/RESULTS/HOST/TRACKING_METHOD	(VALUE, IP_LIST*)
/HOST_LIST/RESULTS/HOST/TRACKING_METHOD/VALUE	(#PCDATA)
	The tracking method of the host for which details are reported. A valid value is "IP address", "DNS hostname", or "NetBIOS hostname".
/HOST_LIST/RESULTS/HOST/DNS	(#PCDATA)
	The DNS host name when known.
/HOST_LIST/RESULTS/HOST/NETBIOS	(#PCDATA)
	The DNS host name if appropriate, when known.

XPath	element specifications / notes
/HOST_LIST/RESULTS/HOST/OPERATING_SYSTEM (#PCDATA)	
	The operating system detected on the host.
/HOST_LIST/RESULTS/HOST/OWNER (FIRSTNAME, LASTNAME, USER_LOGIN, IP_LIST*)	
/HOST_LIST/RESULTS/HOST/OWNER/FIRSTNAME (#PCDATA)	
	The owner's first name.
/HOST_LIST/RESULTS/HOST/OWNER/LASTNAME (#PCDATA)	
	The owner's last name.
/HOST_LIST/RESULTS/HOST/OWNER/USER_LOGIN (#PCDATA)	
	The user login for the owner's Qualys account.
/HOST_LIST/RESULTS/HOST/COMMENT (VALUE, IP_LIST*)	
/HOST_LIST/RESULTS/HOST/COMMENT/VALUE (#PCDATA)	
	User-defined host comments for a particular host.
/HOST_LIST/RESULTS/HOST/USER_DEFINED_ATTR_LIST	
	(USER_DEFINED_ATTR+)
/HOST_LIST/RESULTS/HOST/USER_DEFINED_ATTR_LIST/USER_DEFINED_ATTR	
	(UDA_INDEX, UDA_TITLE, UDA_VALUE, IP_LIST*)
/HOST_LIST/RESULTS/HOST/USER_DEFINED_ATTR_LIST/USER_DEFINED_ATTR/UDA_INDEX (#PCDATA)	
	The index number associated with a user-defined host attribute.
/HOST_LIST/RESULTS/HOST/USER_DEFINED_ATTR_LIST/USER_DEFINED_ATTR/UDA_TITLE (#PCDATA)	
	The title of a user-defined attribute.
/HOST_LIST/RESULTS/HOST/USER_DEFINED_ATTR_LIST/USER_DEFINED_ATTR/UDA_VALUE (#PCDATA)	
	The value of a user-defined attribute.
/HOST_LIST/NO_RESULTS	(ERROR | (COMMENT_LIST?, OWNER_LIST?, USER_DEFINED_ATTR_LIST?, TRACKING_METHOD_LIST?))
/HOST_LIST/NO_RESULTS/COMMENT_LIST (COMMENT+)	
/HOST_LIST/NO_RESULTS/COMMENT_LIST/COMMENT (VALUE, IP_LIST*)	
/HOST_LIST/RESULTS/COMMENT_LIST/COMMENT/VALUE (#PCDATA)	
	Host comments for which host details are reported.
/HOST_LIST/NO_RESULTS/OWNER_LIST (OWNER+)	
/HOST_LIST/NO_RESULTS/OWNER_LIST/OWNER	
	(FIRSTNAME, LASTNAME, USER_LOGIN, IP_LIST*)
/HOST_LIST/NO_RESULTS/OWNER_LIST/OWNER/FIRSTNAME (#PCDATA)	
	The first name of an asset owner, for which host details are reported.
/HOST_LIST/NO_RESULTS/OWNER_LIST/OWNER/LASTNAME (#PCDATA)	
	The last name of an asset owner, for which host details are reported.
/HOST_LIST/NO_RESULTS/OWNER_LIST/OWNER/USER_LOGIN (#PCDATA)	
	The Qualys user login for the asset owner, for which host details are reported.

XPath	element specifications / notes
/HOST_LIST/NO_RESULTS/TRACKING_METHOD_LIST	(TRACKING_METHOD+)
/HOST_LIST/NO_RESULTS/TRACKING_METHOD_LIST /TRACKING_METHOD	(VALUE, IP_LIST*)
/HOST_LIST/NO_RESULTS/TRACKING_METHOD_LIST /TRACKING_METHOD/VALUE	(#PCDATA)
	The tracking methods for which host details are reported.

Asset Domain List

The asset domain list is an XML report is returned from the **asset_domain_list.php** function and the **domain_list.php** function. This report includes information about the domains in the subscription.

The asset domain list DTD and XPaths are described below.

DTD for Asset Domain List

A recent DTD for the asset domain list (domain_list.dtd) is shown below.

```
<!-- QUALYS DOMAIN LIST DTD -->

<!ELEMENT DOMAIN (DOMAIN_NAME, NETBLOCK?)>
<!ELEMENT DOMAIN_LIST (DOMAIN*)>
<!ELEMENT DOMAIN_NAME (#PCDATA)>
<!ELEMENT NETBLOCK (RANGE+)>
<!ELEMENT RANGE (START, END)>
<!ELEMENT START (#PCDATA)>
<!ELEMENT END (#PCDATA)>
```

XPaths for Asset Domain List

This section describes the XPaths for the domain list (domain_list.dtd).

XPath	element specifications / notes
/DOMAIN	(DOMAIN_NAME, NETBLOCK?)
/DOMAIN/DOMAIN_LIST	(DOMAIN*)
/DOMAIN/DOMAIN_LIST/DOMAIN_NAME	(#PCDATA) A domain name.
/DOMAIN/DOMAIN_LIST/NETBLOCK	(RANGE+)
/DOMAIN/DOMAIN_LIST/NETBLOCK/RANGE	(START, END)
/DOMAIN/DOMAIN_LIST/NETBLOCK/RANGE/START	(#PCDATA) An IP address that represents the start of a netblock range that is defined for the domain.
/DOMAIN/DOMAIN_LIST/NETBLOCK/RANGE/END	(#PCDATA) An IP address that represents the end of a netblock range that is defined for the domain.

Asset Group List

The asset group list is an XML report is returned from the **`asset_group_list.php`** function. This report includes information about asset groups in the user account.

The asset group list DTD and XPaths are described below.

DTD for Asset Group List

A recent DTD for the asset group list (asset_group_list.dtd) is shown below.

```
<!-- QUALYS ASSET GROUP LIST DTD -->

<!ELEMENT ASSET_GROUP_LIST (ASSET_GROUP*|ERROR)>
<!ELEMENT ASSET_GROUP (ID, TITLE, SCANIPS?, SCANDNS?, SCANNETBIOS?,
      MAPDOMAINS?, SCANNER_APPLIANCES?, COMMENTS?, BUSINESS_IMPACT,
      DIVISION?, FUNCTION?, LOCATION?, CVSS_ENVIRO_CDP?, CVSS_ENVIRO_TD?,
      CVSS_ENVIRO_CR?, CVSS_ENVIRO_IR?, CVSS_ENVIRO_AR?, LAST_UPDATE,
      ASSIGNED_USERS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT SCANIPS (IP+)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT SCANDNS (DNS+)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT SCANNETBIOS (NETBIOS+)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT MAPDOMAINS (DOMAIN+)>
<!ELEMENT DOMAIN (#PCDATA)>
<!ATTLIST DOMAIN
          netblock CDATA #IMPLIED
>
<!ELEMENT SCANNER_APPLIANCE
(SCANNER_APPLIANCE_NAME,SCANNER_APPLIANCE_SN+)>
<!ELEMENT SCANNER_APPLIANCES (SCANNER_APPLIANCE*)>
<!ELEMENT SCANNER_APPLIANCE_NAME (#PCDATA)>
<!ELEMENT SCANNER_APPLIANCE_SN (#PCDATA)>
<!ATTLIST SCANNER_APPLIANCE
          asset_group_default CDATA #IMPLIED
>
<!ELEMENT COMMENTS (#PCDATA)>

<!ELEMENT BUSINESS_IMPACT (RANK,IMPACT_TITLE)>
<!ELEMENT RANK (#PCDATA)>
<!ELEMENT IMPACT_TITLE (#PCDATA)>

<!ELEMENT DIVISION (#PCDATA)>
<!ELEMENT FUNCTION (#PCDATA)>
```

```
<!ELEMENT LOCATION (#PCDATA)>
<!ELEMENT CVSS_ENVIRO_CDP (#PCDATA)>
<!ELEMENT CVSS_ENVIRO_TD (#PCDATA)>
<!ELEMENT CVSS_ENVIRO_CR (#PCDATA)>
<!ELEMENT CVSS_ENVIRO_IR (#PCDATA)>
<!ELEMENT CVSS_ENVIRO_AR (#PCDATA)>
<!ELEMENT LAST_UPDATE (#PCDATA)>
<!ELEMENT ASSIGNED_USERS (ASSIGNED_USER+)>
<!ELEMENT ASSIGNED_USER (LOGIN, FIRSTNAME, LASTNAME, ROLE)>
<!ELEMENT LOGIN (#PCDATA)>
<!ELEMENT FIRSTNAME (#PCDATA)>
<!ELEMENT LASTNAME (#PCDATA)>
<!ELEMENT ROLE (#PCDATA)>

<!ELEMENT ERROR (#PCDATA)*>
<!ATTLIST ERROR number CDATA #IMPLIED>
<!-- EOF -->
```

XPaths for Asset Group List

This section describes the XPaths for the asset group list (asset_group_list.dtd).

XPath	element specifications / notes
/ASSET_GROUP_LIST	(ASSET_GROUP*|ERROR)
/ASSET_GROUP_LIST/ASSET_GROUP	(ID, TITLE, SCANIPS?, SCANDNS?, SCANNETBIOS?, MAPDOMAINS?, SCANNER_APPLIANCES?, COMMENTS?, BUSINESS_IMPACT, DIVISION?, FUNCTION?, LOCATION?, CVSS_ENVIRO_CDP?, CVSS_ENVIRO_TD?, CVSS_ENVIRO_CR?, CVSS_ENVIRO_IR?, CVSS_ENVIRO_AR?, LAST_UPDATE, ASSIGNED_USERS?)
/ASSET_GROUP_LIST/ASSET_GROUP/ID (#PCDATA)	Asset group ID.
/ASSET_GROUP_LIST/ASSET_GROUP/TITLE (#PCDATA)	Asset group title.
/ASSET_GROUP_LIST/ASSET_GROUP/SCANIPS (IP+)	
/ASSET_GROUP_LIST/ASSET_GROUP/SCANIPS/IP (#PCDATA)	IP address or IP address range in the asset group.
/ASSET_GROUP_LIST/ASSET_GROUP/SCANDNS (DNS+)	
/ASSET_GROUP_LIST/ASSET_GROUP/SCANDNS/DNS (#PCDATA)	DNS hostname in the asset group, used to scan by hostname.
/ASSET_GROUP_LIST/ASSET_GROUP/SCANNETBIOS (NETBIOS+)	
/ASSET_GROUP_LIST/ASSET_GROUP/SCANNETBIOS/NETBIOS (#PCDATA)	NetBIOS hostname in the asset group, used to scan by hostname.

XPath	element specifications / notes
/ASSET_GROUP_LIST/ASSET_GROUP/MAPDOMAINS (DOMAIN+)	
/ASSET_GROUP_LIST/ASSET_GROUP/MAPDOMAINS/DOMAIN (#PCDATA)	
	Domain name in the asset group.
attribute: **netblock**	**netblock** is *implied* and, if present, is the netblock defined for the domain name.
/ASSET_GROUP_LIST/ASSET_GROUP/SCANNER_APPLIANCES (SCANNER_APPLIANCE*)	
/ASSET_GROUP_LIST/ASSET_GROUP/SCANNER_APPLIANCES/SCANNER_APPLIANCE (SCANNER_APPLIANCE_NAME,SCANNER_APPLIANCE_SN+)	
attribute: **asset_group_default**	**asset_group_default** is *implied* and, if present, indicates whether the scanner appliance is the default scanner in the asset group.
/ASSET_GROUP_LIST/ASSET_GROUP/SCANNER_APPLIANCES/SCANNER_APPLIANCE/SCANNER_APPLIANCE_NAME (#PCDATA)	
	Name of a scanner appliance in the asset group.
/ASSET_GROUP_LIST/ASSET_GROUP/SCANNER_APPLIANCES/SCANNER_APPLIANCE/SCANNER_APPLIANCE_SN (#PCDATA)	
	The serial number of a scanner appliance.
/ASSET_GROUP_LIST/ASSET_GROUP/COMMENTS (#PCDATA)	
	The comments defined for the asset group.
/ASSET_GROUP_LIST/ASSET_GROUP/BUSINESS_IMPACT (RANK, IMPACT_TITLE)	
/ASSET_GROUP_LIST/ASSET_GROUP/BUSINESS_IMPACT/RANK (#PCDATA)	
	The rank of the business impact level as defined for the asset group's business information. When Qualys provided levels are used, a valid value is an integer from 1 to 5 where 5 represents the highest level.
/ASSET_GROUP_LIST/ASSET_GROUP/BUSINESS_IMPACT/IMPACT_TITLE (#PCDATA)	
	The title of the business impact level as defined for the asset group's business information. When Qualys provided levels are used, a valid value is a title string: Critical (rank 5), High (rank 4), Medium (rank 3), Minor (rank 2), or Low (rank 1).
/ASSET_GROUP_LIST/ASSET_GROUP/DIVISION (#PCDATA)	
	The division defined for the asset group's business information.
/ASSET_GROUP_LIST/ASSET_GROUP/FUNCTION (#PCDATA)	
	The function defined for the asset group's business information.
/ASSET_GROUP_LIST/ASSET_GROUP/LOCATION (#PCDATA)	
	The location defined for the asset group's business information.
/ASSET_GROUP_LIST/ASSET_GROUP/CVSS_ENVIRO_CDP (#PCDATA)	
	The setting for the CVSS Environmental Metric: Collateral Damage Potential as defined for the asset group. For the "All" asset group, the service automatically sets the metric value to High.
/ASSET_GROUP_LIST/ASSET_GROUP/CVSS_ENVIRO_TD (#PCDATA)	
	The setting for the CVSS Environmental Metric: Target Distribution as defined for the asset group. For the "All" asset group, the service automatically sets the metric value to High.

XPath	element specifications / notes
/ASSET_GROUP_LIST/ASSET_GROUP/CVSS_ENVIRO_CR (#PCDATA)	
	The setting for the CVSS Environmental Metric: Confidentiality Requirement as defined for the asset group. For the "All" asset group, the service automatically sets the metric value to Not Defined.
/ASSET_GROUP_LIST/ASSET_GROUP/CVSS_ENVIRO_IR (#PCDATA)	
	The setting for the CVSS Environmental Metric: Integrity Requirement as defined for the asset group. For the "All" asset group, the service automatically sets the metric value to Not Defined.
/ASSET_GROUP_LIST/ASSET_GROUP/CVSS_ENVIRO_AR (#PCDATA)	
	The setting for the CVSS Environmental Metric: Availability Requirement as defined for the asset group. For the "All" asset group, the service automatically sets the metric value to Not Defined.
/ASSET_GROUP_LIST/ASSET_GROUP/LAST_UPDATE (#PCDATA)	
	The date and time when the asset group was last updated, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/ASSET_GROUP_LIST/ASSET_GROUP/ASSIGNED_USERS (ASSIGNED_USER+)	
/ASSET_GROUP_LIST/ASSET_GROUP/ASSIGNED_USERS/ASSIGNED_USER	
	(LOGIN, FIRSTNAME, LASTNAME, ROLE)
/ASSET_GROUP_LIST/ASSET_GROUP/ASSIGNED_USERS/ASSIGNED_USER/LOGIN (#PCDATA)	
	The login of the user account that owns the asset group.
/ASSET_GROUP_LIST/ASSET_GROUP/ASSIGNED_USERS/ASSIGNED_USER/FIRSTNAME (#PCDATA)	
	The first name of the user account that owns the asset group.
/ASSET_GROUP_LIST/ASSET_GROUP/ASSIGNED_USERS/ASSIGNED_USER/LASTNAME (#PCDATA)	
	The last name of the user account that owns the asset group.
/ASSET_GROUP_LIST/ASSET_GROUP/ASSIGNED_USERS/ASSIGNED_USER/ROLE (#PCDATA)	
	The user role associated with the user account that owns the asset group.
/ASSET_GROUP_LIST/ERROR (#PCDATA)	
attribute: **number**	**number** is *implied* and if present, will be an error code.

Asset Search Report

The asset search report is an XML report is returned from the **asset_search.php** function. The asset search report includes information about hosts in the user account that have been scanned.

The asset search report DTD and XPaths are described below.

DTD for Asset Search Report

A recent DTD for the asset search report (asset_search_report.dtd) is shown below.

```
<!-- QUALYS ASSET SEARCH REPORT DTD -->

<!ELEMENT ASSET_SEARCH_REPORT (ERROR | (HEADER, HOST_LIST?))>

<!ELEMENT ERROR (#PCDATA)*>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!-- HEADER -->

<!ELEMENT HEADER (COMPANY, USERNAME, GENERATION_DATETIME, FILTERS)>

<!ELEMENT COMPANY (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT GENERATION_DATETIME (#PCDATA)>
<!ELEMENT FILTERS
((IP_LIST|ASSET_GROUPS|ASSET_TAGS|FILTER_DNS|FILTER_NETBIOS|TRACKING_METH
OD|FILTER_OPERATING_SYSTEM|FILTER_OS_CPE|FILTER_PORT|
FILTER_SERVICE|FILTER_QID|FILTER_RESULT|FILTER_LAST_SCAN_DATE)+)>

<!ELEMENT IP_LIST (RANGE*)>
<!ELEMENT RANGE (START, END)>
<!ELEMENT START (#PCDATA)>
<!ELEMENT END (#PCDATA)>

<!ELEMENT ASSET_GROUPS (ASSET_GROUP_TITLE+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>

<!ELEMENT ASSET_TAGS (INCLUDED_TAGS, EXCLUDED_TAGS?)>

<!ELEMENT INCLUDED_TAGS (ASSET_TAG*)>
<!ATTLIST INCLUDED_TAGS scope CDATA #IMPLIED>

<!ELEMENT EXCLUDED_TAGS (ASSET_TAG*)>
<!ATTLIST EXCLUDED_TAGS scope CDATA #IMPLIED>

<!ELEMENT ASSET_TAG (#PCDATA)>
```

```
<!ELEMENT FILTER_DNS (#PCDATA)>
<!ATTLIST FILTER_DNS criterion CDATA #IMPLIED>

<!ELEMENT FILTER_NETBIOS (#PCDATA)>
<!ATTLIST FILTER_NETBIOS criterion CDATA #IMPLIED>

<!ELEMENT TRACKING_METHOD (#PCDATA)>

<!ELEMENT FILTER_OPERATING_SYSTEM (#PCDATA)>
<!ATTLIST FILTER_OPERATING_SYSTEM criterion CDATA #IMPLIED>
<!ELEMENT FILTER_OS_CPE (#PCDATA)>
<!ELEMENT FILTER_PORT (#PCDATA)>
<!ELEMENT FILTER_SERVICE (#PCDATA)>
<!ELEMENT FILTER_QID (#PCDATA)>
<!ELEMENT FILTER_RESULT (#PCDATA)>
<!ATTLIST FILTER_RESULT criterion CDATA #IMPLIED>
<!ELEMENT FILTER_LAST_SCAN_DATE (#PCDATA)>
<!ATTLIST FILTER_LAST_SCAN_DATE criterion CDATA #IMPLIED>

<!-- HOST_LIST -->

<!ELEMENT HOST_LIST ((HOST|WARNING)+)>

<!ELEMENT HOST (ERROR | (IP, HOST_TAGS?,TRACKING_METHOD,
                         DNS?, NETBIOS?, OPERATING_SYSTEM?, OS_CPE?,
                         QID_LIST?, PORT_SERVICE_LIST?,
                         ASSET_GROUPS?, LAST_SCAN_DATE?))>

<!ELEMENT IP (#PCDATA)>
<!ELEMENT HOST_TAGS (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT OPERATING_SYSTEM (#PCDATA)>
<!ELEMENT OS_CPE (#PCDATA)>
<!ELEMENT QID_LIST (QID+)>
<!ELEMENT QID (ID, RESULT?)>
<!ELEMENT ID (#PCDATA)>
<!-- if format is set to "table" -->
<!-- tab '\t' is the col separator -->
<!-- and new line '\n' is the end of row -->
<!ELEMENT RESULT (#PCDATA)>
<!ATTLIST RESULT
    format CDATA #IMPLIED
>
<!ELEMENT PORT_SERVICE_LIST (PORT_SERVICE+)>
<!ELEMENT PORT_SERVICE (PORT,SERVICE)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT SERVICE (#PCDATA)>
```

```
<!ELEMENT LAST_SCAN_DATE (#PCDATA)>

<!ELEMENT WARNING (#PCDATA)>
<!ATTLIST WARNING number CDATA #IMPLIED>
```

XPaths for Asset Search Report

This section describes the XPaths for the asset search report (asset_search_report.dtd).

XPath	element specifications / notes
/ASSET_SEARCH_REPORT	(ERROR | (HEADER, HOST_LIST?))
/ASSET_SEARCH_REPORT/ERROR	(#PCDATA)
attribute: **number**	**number** is *implied* and if present, will be an error code.
/ASSET_SEARCH_REPORT/HEADER	(COMPANY, USERNAME, GENERATION_DATETIME, FILTERS)
/ASSET_SEARCH_REPORT/HEADER/COMPANY (#PCDATA)	The company name.
/ASSET_SEARCH_REPORT/HEADER/USERNAME (#PCDATA)	The login ID for the account used to request the asset search.
/ASSET_SEARCH_REPORT/HEADER/GENERATION_DATETIME (#PCDATA)	The date and time when the report was generated, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/ASSET_SEARCH_REPORT/HEADER/FILTERS	((IP_LIST | ASSET_GROUPS | ASSET_TAGS | FILTER_DNS | FILTER_NETBIOS | TRACKING_METHOD | FILTER_OPERATING_SYSTEM | FILTER_OS_CPE | FILTER_PORT | FILTER_SERVICE | FILTER_QID | FILTER_RESULT | FILTER_LAST_SCAN_DATE)+)
/ASSET_SEARCH_REPORT/HEADER/FILTERS/IP_LIST (RANGE*)	
/ASSET_SEARCH_REPORT/HEADER/FILTERS/IP_LIST/RANGE (START, END)	
/ASSET_SEARCH_REPORT/HEADER/FILTERS/IP_LIST/RANGE/START (#PCDATA)	An IP address identifying the start of an IP range specified for the search target.
/ASSET_SEARCH_REPORT/HEADER/FILTERS/IP_LIST/RANGE/END (#PCDATA)	An IP address identifying the end of an IP range specified for the search target.
/ASSET_SEARCH_REPORT/HEADER/FILTERS/ASSET_GROUPS (ASSET_GROUP_TITLE+)	
/ASSET_SEARCH_REPORT/HEADER/FILTERS/ASSET_GROUPS/ASSET_GROUP_TITLE (#PCDATA)	An asset group title specified for the search target.

XPath	element specifications / notes
/ASSET_SEARCH_REPORT/HEADER/FILTERS/ASSET_GROUPS/ASSET_TAGS (INCLUDED_TAGS, EXCLUDED_TAGS?)	
/ASSET_SEARCH_REPORT/HEADER/FILTERS/ASSET_GROUPS/ASSET_TAGS/INCLUDED_TAGS/ ASSET_TAG (#PCDATA)	
	The list of asset tags included in the search target. The scope "all" means hosts matching all tags; scope "any" means hosts matching at least one of the tags.
/ASSET_SEARCH_REPORT/HEADER/FILTERS/ASSET_GROUPS/ASSET_TAGS/EXCLUDED_TAGS / ASSET_TAG (#PCDATA)	
	The list of asset tags excluded from the search target. The scope "all" means hosts matching all tags; scope "any" means hosts matching at least one of the tags.
/ASSET_SEARCH_REPORT/HEADER/FILTERS/FILTER_DNS (#PCDATA)	
	A DNS host name string specified for the search target.
attribute: **criterion**	**criterion** is *implied* and if present, indicates the match prefix specified for the DNS host name string: begin, match, contain, or end.
/ASSET_SEARCH_REPORT/HEADER/FILTERS/FILTERN_NETBIOS (#PCDATA)	
	A NetBIOS host name string defined for the search target.
attribute: **criterion**	**criterion** is *implied* and if present, indicates the match prefix specified for the NetBIOS host name string: begin, match, contain, or end.
/ASSET_SEARCH_REPORT/HEADER/FILTERS/TRACKING_METHOD (#PCDATA)	
	A tracking method specified as a search attribute. A valid value is "ip", "dns", or "netbios".
/ASSET_SEARCH_REPORT/HEADER/FILTERS/FILTER_OPERATING_SYSTEM (#PCDATA)	
	Operating system names specified as a search attribute.
attribute: **criterion**	**criterion** is *implied* and, if present, indicates the match prefix for the specified operating systems: begin, match, contain, or end.
/ASSET_SEARCH_REPORT/HEADER/FILTERS/FILTER_OS_CPE (#PCDATA)	
	OS CPE name specified as a search attribute. (It's possible to search by OS CPE name when the OS CPE feature is enabled for the subscription, and an authenticated scan was run on target hosts after enabling this feature.)
/ASSET_SEARCH_REPORT/HEADER/FILTERS/FILTER_PORT (#PCDATA)	
	Port numbers specified as a search attribute.
/ASSET_SEARCH_REPORT/HEADER/FILTERS/FILTER_SERVICE (#PCDATA)	
	Service names specified as a search attribute.
/ASSET_SEARCH_REPORT/HEADER/FILTERS/FILTER_QID (#PCDATA)	
	QIDs specified as a search attribute.
/ASSET_SEARCH_REPORT/HEADER/FILTERS/FILTER_RESULT (#PCDATA)	
	A text string in vulnerability test results specified as a search attribute.
attribute: **criterion**	**criterion** is *implied* and, if present, indicates the match prefix specified for the vulnerability test results: begin, match, contain or end.

XPath	element specifications / notes
/ASSET_SEARCH_REPORT/HEADER/FILTERS/FILTER_LAST_SCAN_DATE (#PCDATA)	
	The last scan date specified as a search attribute, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
attribute: **criterion**	**criterion** is *implied* and, if present, indicates the match prefix specified for the last scan date: within or not_within.
/ASSET_SEARCH_REPORT/HOST_LIST ((HOST|WARNING)+)	
/ASSET_SEARCH_REPORT/HOST_LIST/HOST	
	(ERROR | (IP, HOST_TAGS?, TRACKING_METHOD, DNS?, NETBIOS?, OPERATING_SYSTEM?, OS _CPE?, QID_LIST?, PORT_SERVICE_LIST?, ASSET_GROUPS?, LAST_SCAN_DATE?))
/ASSET_SEARCH_REPORT/HOST_LIST/HOST/IP (#PCDATA)	
	The IP address of a host.
/ASSET_SEARCH_REPORT/HOST_LIST/HOST/HOST_TAGS (#PCDATA)	
	The tags assigned to the host.
/ASSET_SEARCH_REPORT/HOST_LIST/HOST/TRACKING_METHOD (#PCDATA)	
	The tracking method assigned to a host.
/ASSET_SEARCH_REPORT/HOST_LIST/HOST/DNS (#PCDATA)	
	The DNS host name of a host.
/ASSET_SEARCH_REPORT/HOST_LIST/HOST/NETBIOS (#PCDATA)	
	The NetBIOS name of a host.
/ASSET_SEARCH_REPORT/HOST_LIST/HOST/OPERATING_SYSTEM (#PCDATA)	
	The operating system detected on the host.
/ASSET_SEARCH_REPORT/HOST_LIST/HOST/OS_CPE (#PCDATA)	
	The OS CPE name assigned to the operating system detected on the host. (The OS CPE name appears only when the OS CPE feature is enabled for the subscription, and an authenticated scan was run on this host after enabling this feature.)
/ASSET_SEARCH_REPORT/HOST_LIST/HOST/QID_LIST (QID+)	
/ASSET_SEARCH_REPORT/HOST_LIST/HOST/QID_LIST/QID (ID, RESULT?)	
/ASSET_SEARCH_REPORT/HOST_LIST/HOST/QID_LIST/QID/ID (#PCDATA)	
	The QID of a vulnerability detected on the host. This appears only when QIDs are specified as a search filter.
/ASSET_SEARCH_REPORT/HOST_LIST/HOST/QID_LIST/QID/RESULT (#PCDATA)	
	Specific scan test results for the vulnerability, from the host assessment data.
attribute: **format**	**format** is *implied* and if present, will be "table," indicating that the results are a table that has columns separated by tabulation characters and rows separated by new-line characters
/ASSET_SEARCH_REPORT/HOST_LIST/HOST/PORT_SERVICE_LIST (PORT_SERVICE+)	
/ASSET_SEARCH_REPORT/HOST_LIST/HOST/PORT_SERVICE_LIST/PORT_SERVICE	
	(PORT, SERVICE)

XPath	element specifications / notes
/ASSET_SEARCH_REPORT/HOST_LIST/HOST/PORT_SERVICE_LIST/PORT	
	(#PCDATA)
	The number of an open port detected on the host. This port is associated with the service in the <SERVICE> element which is inside the same <PORT_SERVICE> element. Note: This element appears only when the "vuln_port" and/or "vuln_service" input parameters are specified for the asset search request.
/ASSET_SEARCH_REPORT/HOST_LIST/HOST/PORT_SERVICE_LIST/PORT_SERVICE/SERVICE	
	(#PCDATA)
	The name of a service found to be running on the host. This service is associated with the port number in the <PORT> element which is inside the same <PORT_SERVICE> element. Note: This element appears only when the "vuln_port" and/or "vuln_service" input parameters are specified for the asset search request.
/ASSET_SEARCH_REPORT/HOST_LIST/HOST/ASSET_GROUPS (ASSET_GROUP_TITLE+)	
/ASSET_SEARCH_REPORT/HOST_LIST/HOST/ASSET_GROUPS/ASSET_GROUP_TITLE (#PCDATA)	
	The title of an asset group to which the host belongs.
/ASSET_SEARCH_REPORT/HOST_LIST/HOST/LAST_SCAN_DATE (#PCDATA)	
	The date and time when the host was last scanned, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/ASSET_SEARCH_REPORT/HOST_LIST/WARNING (#PCDATA)	
attribute: **number**	**number** is *implied* and if present, will be a warning code.

Empty Asset Search Results

The sample asset search report shown below was returned from this URL:

```
https://qualysapi.qualys.com/msp/asset_search.php?
target_asset_groups=Dallas&tracking_method=netbios
```

This request searched for hosts in the asset group “Dallas” that are tracked by NetBIOS host name. The search report is empty since no hosts were found to match the search criteria.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE ASSET_SEARCH_REPORT SYSTEM
"https://qualysapi.qualys.com/asset_search_report.dtd">
<ASSET_SEARCH_REPORT>
  <HEADER>
    <COMPANY><![CDATA[Acme]]></COMPANY>
    <USERNAME>acme_bb</USERNAME>
    <GENERATION_DATETIME>2007-10-20T20:08:07Z</GENERATION_DATETIME>
    <FILTERS>
      <ASSET_GROUPS>
        <ASSET_GROUP_TITLE><![CDATA[Dallas]]></ASSET_GROUP_TITLE>
      </ASSET_GROUPS>
      <TRACKING_METHOD>netbios</TRACKING_METHOD>
    </FILTERS>
  </HEADER>
</ASSET_SEARCH_REPORT>
```

Asset Range Info Report

The asset range info report is an XML report is returned from the **`asset_range_info.php`** function. This asset report includes information about hosts in the user account that have been scanned based on target hosts (IP addresses and/or asset groups) specified as a part of the report request.

The DTD for the asset range info report is very similar to the asset data report, with these slight differences: 1) The header section in the asset range info report includes the company name, user login, report generation time and target hosts, and 2) There are no appendices in the asset range info report, and 3) The glossary section always includes Exploitability information for vulnerabilities, when this information is available in the KnowledgeBase.

The elements in the asset range info report also appear in the asset data report, with the exceptions noted above. For a reference of report elements and XPaths, refer to "Asset Data Report" earlier in this appendix.

DTD for Asset Range Info Report

A recent DTD for the asset range info report (asset_range_info.dtd) is shown below.

```
<!-- QUALYS ASSET RANGE INFO DTD -->

<!ELEMENT ASSET_RANGE_INFO (ERROR | (HEADER, HOST_LIST?, GLOSSARY?))>

<!ELEMENT ERROR (#PCDATA)*>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!-- HEADER -->

<!ELEMENT HEADER (COMPANY, USERNAME, GENERATION_DATETIME, TARGET)>

<!ELEMENT COMPANY (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT GENERATION_DATETIME (#PCDATA)>
<!ELEMENT TARGET (USER_ASSET_GROUPS?, USER_IP_LIST?, COMBINED_IP_LIST)>

<!ELEMENT USER_ASSET_GROUPS (ASSET_GROUP_TITLE+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>

<!ELEMENT USER_IP_LIST (RANGE*)>
<!ELEMENT RANGE (START, END)>
<!ELEMENT START (#PCDATA)>
<!ELEMENT END (#PCDATA)>

<!ELEMENT COMBINED_IP_LIST (RANGE*)>
```

```
<!-- HOST_LIST -->

<!ELEMENT HOST_LIST (HOST+)>

<!ELEMENT HOST (ERROR | (IP, TRACKING_METHOD,
                         DNS?, NETBIOS?, OPERATING_SYSTEM?,
                         ASSET_GROUPS?, VULN_INFO_LIST?))>

<!ELEMENT IP (#PCDATA)>
<!ELEMENT TRACKING_METHOD (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT OPERATING_SYSTEM (#PCDATA)>
<!ELEMENT ASSET_GROUPS (ASSET_GROUP_TITLE+)>
<!ELEMENT VULN_INFO_LIST (VULN_INFO+)>

<!ELEMENT VULN_INFO (QID, TYPE, PORT?, SERVICE?, FQDN?, PROTOCOL?, SSL?,
                     RESULT?, FIRST_FOUND?, LAST_FOUND?, TIMES_FOUND?,
                     VULN_STATUS?, TICKET_NUMBER?, TICKET_STATE?)>

<!ELEMENT QID (#PCDATA)>
<!ATTLIST QID id IDREF #REQUIRED>

<!ELEMENT TYPE (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT SERVICE (#PCDATA)>
<!ELEMENT FQDN (#PCDATA)>
<!ELEMENT PROTOCOL (#PCDATA)>
<!ELEMENT SSL (#PCDATA)>

<!ELEMENT RESULT (#PCDATA)>
<!ATTLIST RESULT format CDATA #IMPLIED>

<!ELEMENT FIRST_FOUND (#PCDATA)>
<!ELEMENT LAST_FOUND (#PCDATA)>
<!ELEMENT TIMES_FOUND (#PCDATA)>
<!-- Note: VULN_STATUS is N/A for IGs -->
<!ELEMENT VULN_STATUS (#PCDATA)>

<!ELEMENT TICKET_NUMBER (#PCDATA)>
<!ELEMENT TICKET_STATE (#PCDATA)>


<!-- GLOSSARY -->

<!ELEMENT GLOSSARY (VULN_DETAILS_LIST)>

<!ELEMENT VULN_DETAILS_LIST (VULN_DETAILS+)>
```

```
<!ELEMENT VULN_DETAILS (QID, TITLE, SEVERITY, CATEGORY,
                        CUSTOMIZED?, THREAT, THREAT_COMMENT?, IMPACT,
                        IMPACT_COMMENT?,
                        SOLUTION, SOLUTION_COMMENT?, COMPLIANCE?,
                        CORRELATION?, LAST_UPDATE?,
                        CVSS_SCORE?, VENDOR_REFERENCE_LIST?,
                        CVE_ID_LIST?, BUGTRAQ_ID_LIST?)>
<!ATTLIST VULN_DETAILS id ID #REQUIRED>

<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT SEVERITY (#PCDATA)>
<!ELEMENT CATEGORY (#PCDATA)>

<!ELEMENT CUSTOMIZED (CUSTOM_SEVERITY)>
<!ELEMENT CUSTOM_SEVERITY (#PCDATA)>

<!ELEMENT THREAT (#PCDATA)>
<!ELEMENT THREAT_COMMENT (#PCDATA)>
<!ELEMENT IMPACT (#PCDATA)>
<!ELEMENT IMPACT_COMMENT (#PCDATA)>
<!ELEMENT SOLUTION (#PCDATA)>
<!ELEMENT SOLUTION_COMMENT (#PCDATA)>

<!ELEMENT COMPLIANCE (COMPLIANCE_INFO+)>
<!ELEMENT COMPLIANCE_INFO (COMPLIANCE_TYPE, COMPLIANCE_SECTION,
                           COMPLIANCE_DESCRIPTION)>
<!ELEMENT COMPLIANCE_TYPE (#PCDATA)>
<!ELEMENT COMPLIANCE_SECTION (#PCDATA)>
<!ELEMENT COMPLIANCE_DESCRIPTION (#PCDATA)>

<!ELEMENT CORRELATION (EXPLOITABILITY?,MALWARE?)>
<!ELEMENT EXPLOITABILITY (EXPLT_SRC)+>
<!ELEMENT EXPLT_SRC (SRC_NAME, EXPLT_LIST)>
<!ELEMENT SRC_NAME (#PCDATA)>
<!ELEMENT EXPLT_LIST (EXPLT)+>
<!ELEMENT EXPLT (REF, DESC, LINK?)>
<!ELEMENT REF (#PCDATA)>
<!ELEMENT DESC (#PCDATA)>
<!ELEMENT LINK (#PCDATA)>

<!ELEMENT MALWARE (MW_SRC)+>
<!ELEMENT MW_SRC (SRC_NAME, MW_LIST)>
<!ELEMENT MW_LIST (MW_INFO)+>
<!ELEMENT MW_INFO (MW_ID, MW_TYPE?, MW_PLATFORM?, MW_ALIAS?, MW_RATING?,
                   MW_LINK?)>
<!ELEMENT MW_ID (#PCDATA)>
<!ELEMENT MW_TYPE (#PCDATA)>
<!ELEMENT MW_PLATFORM (#PCDATA)>
<!ELEMENT MW_ALIAS (#PCDATA)>
```

```
<!ELEMENT MW_RATING (#PCDATA)>
<!ELEMENT MW_LINK (#PCDATA)>

<!ELEMENT LAST_UPDATE (#PCDATA)>

<!ELEMENT CVSS_SCORE (CVSS_BASE?, CVSS_TEMPORAL?)>
<!ELEMENT CVSS_BASE (#PCDATA)>
<!ATTLIST CVSS_BASE
    source CDATA #IMPLIED
>
<!ELEMENT CVSS_TEMPORAL (#PCDATA)>

<!ELEMENT VENDOR_REFERENCE_LIST (VENDOR_REFERENCE+)>
<!ELEMENT VENDOR_REFERENCE (ID,URL)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT URL (#PCDATA)>

<!ELEMENT CVE_ID_LIST (CVE_ID+)>
<!ELEMENT CVE_ID (ID,URL)>

<!ELEMENT BUGTRAQ_ID_LIST (BUGTRAQ_ID+)>
<!ELEMENT BUGTRAQ_ID (ID,URL)>
```

Asset Data Report

The asset data report is an XML report is returned from the **asset_data_report.php** function. The asset data report includes information about hosts in the user account that have been scanned based on a report template (automatic) specified as a part of the report request.

DTD for Asset Data Report

A recent DTD for the asset data report (asset_data_report.dtd) is shown below.

```
<!-- QUALYS ASSET DATA REPORT DTD -->

<!ELEMENT ASSET_DATA_REPORT (ERROR | (HEADER, RISK_SCORE_PER_HOST?,
                             HOST_LIST?, GLOSSARY?, APPENDICES?))>

<!ELEMENT ERROR (#PCDATA)*>
<!ATTLIST ERROR number CDATA #IMPLIED>


<!-- HEADER -->

<!ELEMENT HEADER (COMPANY, USERNAME, GENERATION_DATETIME, TEMPLATE,
                  TARGET, RISK_SCORE_SUMMARY?)>

<!ELEMENT COMPANY (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT GENERATION_DATETIME (#PCDATA)>
<!ELEMENT TEMPLATE (#PCDATA)>
<!ELEMENT TARGET (USER_ASSET_GROUPS?, USER_IP_LIST?, COMBINED_IP_LIST?,
                  ASSET_TAG_LIST?)>

<!ELEMENT USER_ASSET_GROUPS (ASSET_GROUP_TITLE+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>

<!ELEMENT USER_IP_LIST (NETWORK?, RANGE*)>
<!ELEMENT RANGE (START, END)>
<!ELEMENT START (#PCDATA)>
<!ELEMENT END (#PCDATA)>

<!ELEMENT COMBINED_IP_LIST (NETWORK?, RANGE*)>

<!ELEMENT ASSET_TAG_LIST (INCLUDED_TAGS, EXCLUDED_TAGS?)>

<!ELEMENT INCLUDED_TAGS (ASSET_TAG*)>
<!ATTLIST INCLUDED_TAGS scope CDATA #IMPLIED>
```

```
<!ELEMENT EXCLUDED_TAGS (ASSET_TAG*)>
<!ATTLIST EXCLUDED_TAGS scope CDATA #IMPLIED>

<!-- AVERAGE RISK_SCORE_SUMMARY -->
<!ELEMENT RISK_SCORE_SUMMARY (TOTAL_VULNERABILITIES, AVG_SECURITY_RISK,
                              BUSINESS_RISK)>
<!ELEMENT TOTAL_VULNERABILITIES (#PCDATA)>
<!ELEMENT AVG_SECURITY_RISK (#PCDATA)>
<!ELEMENT BUSINESS_RISK (#PCDATA)>

<!-- RISK_SCORE_PER_HOST -->
<!ELEMENT RISK_SCORE_PER_HOST (HOSTS+)>
<!ELEMENT HOSTS (IP_ADDRESS, NETWORK?, TOTAL_VULNERABILITIES,
                 SECURITY_RISK)>
<!ELEMENT IP_ADDRESS (#PCDATA)>
<!ELEMENT SECURITY_RISK (#PCDATA)>

<!-- HOST_LIST -->

<!ELEMENT HOST_LIST (HOST+)>

<!ELEMENT HOST (ERROR | (IP, NETWORK?, TRACKING_METHOD, ASSET_TAGS?,
                         DNS?, NETBIOS?, OPERATING_SYSTEM?, OS_CPE?,
                         ASSET_GROUPS?, VULN_INFO_LIST?))>

<!ELEMENT IP (#PCDATA)>
<!ELEMENT NETWORK (#PCDATA)>
<!ELEMENT TRACKING_METHOD (#PCDATA)>
<!ELEMENT ASSET_TAGS (ASSET_TAG+)>
<!ELEMENT ASSET_TAG (#PCDATA)>

<!ELEMENT DNS (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT OPERATING_SYSTEM (#PCDATA)>
<!ELEMENT OS_CPE (#PCDATA)>
<!ELEMENT ASSET_GROUPS (ASSET_GROUP_TITLE+)>
<!ELEMENT VULN_INFO_LIST (VULN_INFO+)>

<!ELEMENT VULN_INFO (QID, TYPE, PORT?, SERVICE?, FQDN?, PROTOCOL?, SSL?,
                     INSTANCE?, RESULT?, FIRST_FOUND?, LAST_FOUND?,
                     TIMES_FOUND?, VULN_STATUS?, CVSS_FINAL?,
                     TICKET_NUMBER?, TICKET_STATE?)>

<!ELEMENT QID (#PCDATA)>
<!ATTLIST QID id IDREF #REQUIRED>

<!ELEMENT TYPE (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT SERVICE (#PCDATA)>
```

```
<!ELEMENT FQDN (#PCDATA)>
<!ELEMENT PROTOCOL (#PCDATA)>
<!ELEMENT SSL (#PCDATA)>

<!ELEMENT RESULT (#PCDATA)>
<!ATTLIST RESULT format CDATA #IMPLIED>

<!ELEMENT FIRST_FOUND (#PCDATA)>
<!ELEMENT LAST_FOUND (#PCDATA)>
<!ELEMENT TIMES_FOUND (#PCDATA)>
<!-- Note: VULN_STATUS is N/A for IGs -->
<!ELEMENT VULN_STATUS (#PCDATA)>

<!ELEMENT CVSS_FINAL (#PCDATA)>
<!ELEMENT TICKET_NUMBER (#PCDATA)>
<!ELEMENT TICKET_STATE (#PCDATA)>

<!ELEMENT INSTANCE (#PCDATA)>

<!-- GLOSSARY -->

<!ELEMENT GLOSSARY (VULN_DETAILS_LIST)>

<!ELEMENT VULN_DETAILS_LIST (VULN_DETAILS+)>

<!ELEMENT VULN_DETAILS (QID, TITLE, SEVERITY, CATEGORY,
                        CUSTOMIZED?, THREAT, THREAT_COMMENT?, IMPACT,
                        IMPACT_COMMENT?, SOLUTION, SOLUTION_COMMENT?,
                        COMPLIANCE?, CORRELATION?, PCI_FLAG,
                        LAST_UPDATE?, CVSS_SCORE?,
                        VENDOR_REFERENCE_LIST?, CVE_ID_LIST?,
                        BUGTRAQ_ID_LIST?)>
<!ATTLIST VULN_DETAILS id ID #REQUIRED>

<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT SEVERITY (#PCDATA)>
<!ELEMENT CATEGORY (#PCDATA)>

<!ELEMENT CUSTOMIZED (DISABLED?, CUSTOM_SEVERITY?)>
<!ELEMENT DISABLED (#PCDATA)>
<!ELEMENT CUSTOM_SEVERITY (#PCDATA)>

<!ELEMENT THREAT (#PCDATA)>
<!ELEMENT THREAT_COMMENT (#PCDATA)>
<!ELEMENT IMPACT (#PCDATA)>
<!ELEMENT IMPACT_COMMENT (#PCDATA)>
<!ELEMENT SOLUTION (#PCDATA)>
<!ELEMENT SOLUTION_COMMENT (#PCDATA)>
<!ELEMENT PCI_FLAG (#PCDATA)>
```

```
<!ELEMENT CORRELATION (EXPLOITABILITY?, MALWARE?)>
<!ELEMENT EXPLOITABILITY (EXPLT_SRC)+>
<!ELEMENT EXPLT_SRC (SRC_NAME, EXPLT_LIST)>
<!ELEMENT SRC_NAME (#PCDATA)>
<!ELEMENT EXPLT_LIST (EXPLT)+>
<!ELEMENT EXPLT (REF, DESC, LINK?)>
<!ELEMENT REF (#PCDATA)>
<!ELEMENT DESC (#PCDATA)>
<!ELEMENT LINK (#PCDATA)>

<!ELEMENT MALWARE (MW_SRC)+>
<!ELEMENT MW_SRC (SRC_NAME, MW_LIST)>
<!ELEMENT MW_LIST (MW_INFO)+>
<!ELEMENT MW_INFO (MW_ID, MW_TYPE?, MW_PLATFORM?, MW_ALIAS?, MW_RATING?,
                   MW_LINK?)>
<!ELEMENT MW_ID (#PCDATA)>
<!ELEMENT MW_TYPE (#PCDATA)>
<!ELEMENT MW_PLATFORM (#PCDATA)>
<!ELEMENT MW_ALIAS (#PCDATA)>
<!ELEMENT MW_RATING (#PCDATA)>
<!ELEMENT MW_LINK (#PCDATA)>

<!ELEMENT LAST_UPDATE (#PCDATA)>

<!ELEMENT CVSS_SCORE (CVSS_BASE?, CVSS_TEMPORAL?)>
<!ELEMENT CVSS_BASE (#PCDATA)>
<!ATTLIST CVSS_BASE
    source CDATA #IMPLIED
>
<!ELEMENT CVSS_TEMPORAL (#PCDATA)>

<!ELEMENT VENDOR_REFERENCE_LIST (VENDOR_REFERENCE+)>
<!ELEMENT VENDOR_REFERENCE (ID,URL)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT URL (#PCDATA)>

<!ELEMENT CVE_ID_LIST (CVE_ID+)>
<!ELEMENT CVE_ID (ID,URL)>

<!ELEMENT BUGTRAQ_ID_LIST (BUGTRAQ_ID+)>
<!ELEMENT BUGTRAQ_ID (ID,URL)>

<!ELEMENT COMPLIANCE (COMPLIANCE_INFO+)>
<!ELEMENT COMPLIANCE_INFO (COMPLIANCE_TYPE, COMPLIANCE_SECTION,
                           COMPLIANCE_DESCRIPTION)>
<!ELEMENT COMPLIANCE_TYPE (#PCDATA)>
<!ELEMENT COMPLIANCE_SECTION (#PCDATA)>
<!ELEMENT COMPLIANCE_DESCRIPTION (#PCDATA)>
```

```
<!-- APPENDICES -->

<!ELEMENT APPENDICES (NO_RESULTS?, NO_VULNS?, TEMPLATE_DETAILS?)>
<!ELEMENT NO_RESULTS (IP_LIST)>
<!ELEMENT IP_LIST (NETWORK?, RANGE*)>
<!ELEMENT NO_VULNS (IP_LIST)>
<!ELEMENT TEMPLATE_DETAILS (VULN_LISTS?, SELECTIVE_VULNS?,
                            EXCLUDED_VULN_LISTS?, EXCLUDED_VULNS?,
                            RESULTING_VULNS?, FILTER_SUMMARY?,
                            EXCLUDED_CATEGORIES?)>
<!ELEMENT VULN_LISTS (#PCDATA)>
<!ELEMENT SELECTIVE_VULNS (#PCDATA)>
<!ELEMENT EXCLUDED_VULN_LISTS (#PCDATA)>
<!ELEMENT EXCLUDED_VULNS (#PCDATA)>
<!ELEMENT RESULTING_VULNS (#PCDATA)>
<!ELEMENT FILTER_SUMMARY (#PCDATA)>
<!ELEMENT EXCLUDED_CATEGORIES (#PCDATA)>
```

XPaths for Asset Data Report

This section describes the XPaths for the asset data report (asset_data_report.dtd).

Report Sections

There are four main sections to the asset data report — Header, Host List, Glossary and Appendices. These sections are summarized below.

XPath	element specifications / notes
/ASSET_DATA_REPORT	(ERROR | (HEADER, RISK_SCORE_PER_HOST?, HOST_LIST?, GLOSSARY?, APPENDICES?))
/ASSET_DATA_REPORT/HEADER	(COMPANY, USERNAME, GENERATION_DATETIME, TEMPLATE, TARGET, RISK_SCORE_SUMMARY?)
	Report summary information.
/ASSET_DATA_REPORT/RISK_SCORE_PER_HOST	(HOSTS+)
	Risk score summary per host. This is included when the report template has the Text Summary setting selected.
/ASSET_DATA_REPORT/HOST_LIST	(HOST+)
	Detected vulnerabilities for each host. For each detected vulnerability, information specific to its detection on the host is also provided.
/ASSET_DATA_REPORT/GLOSSARY	(VULN_DETAILS_LIST)
	Vulnerability information applicable to all hosts.
/ASSET_DATA_REPORT/APPENDICES	(NO_RESULTS?, NO_VULNS?, TEMPLATE_DETAILS?)
	Additional data such as hosts with no scan results and template settings.

XPath	element specifications / notes
/ASSET_DATA_REPORT/ERROR	(#PCDATA)
attribute: **number**	**number** is *implied* and, if present, will be an error code.

Header

XPath	element specifications / notes
/ASSET_DATA_REPORT/HEADER	(COMPANY, USERNAME, GENERATION_DATETIME, TEMPLATE, TARGET, RISK_SCORE_SUMMARY?)
/ASSET_DATA_REPORT/HEADER/COMPANY	(#PCDATA) The company name.
/ASSET_DATA_REPORT/HEADER/USERNAME	(#PCDATA) The login ID for the user who generated the report.
/ASSET_DATA_REPORT/HEADER/GENERATION_DATETIME	(#PCDATA) The date and time when the report was generated, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/ASSET_DATA_REPORT/HEADER/TEMPLATE	(#PCDATA) The title assigned to the template used to generate the report.
/ASSET_DATA_REPORT/HEADER/TARGET	(USER_ASSET_GROUPS?, USER_IP_LIST?, COMBINED_IP_LIST?, ASSET_TAG_LIST?)
/ASSET_DATA_REPORT/HEADER/TARGET/USER_ASSET_GROUPS	(ASSET_GROUP_TITLE+)
/ASSET_DATA_REPORT/HEADER/TARGET/USER_ASSET_GROUPS/ASSET_GROUP_TITLE	(#PCDATA) The title of an asset group that the user specified in the report template.
/ASSET_DATA_REPORT/HEADER/TARGET/USER_IP_LIST	(NETWORK?, RANGE*) The user specified report target.
/ASSET_DATA_REPORT/HEADER/TARGET/USER_IP_LIST/NETWORK	(#PCDATA) The network selected in the report template, when network support is enabled.
/ASSET_DATA_REPORT/HEADER/TARGET/USER_IP_LIST/RANGE	(START, END)
/ASSET_DATA_REPORT/HEADER/TARGET/USER_IP_LIST/RANGE/START	(#PCDATA) The first IP address in a range of IPs that the user specified in the report template.
/ASSET_DATA_REPORT/HEADER/TARGET/USER_IP_LIST/RANGE/END	(#PCDATA) The last IP address in a range of IPs that the user specified in the report template.
/ASSET_DATA_REPORT/HEADER/TARGET/COMBINED_IP_LIST	(NETWORK?, RANGE*) The combined report target.
/ASSET_DATA_REPORT/HEADER/TARGET/COMBINED_IP_LIST/NETWORK	(#PCDATA) The network in the combined report target, when network support is enabled.

XPath	element specifications / notes
/ASSET_DATA_REPORT/HEADER/TARGET/COMBINED_IP_LIST/RANGE (START, END)	
/ASSET_DATA_REPORT/HEADER/TARGET/COMBINED_IP_LIST/RANGE/START (#PCDATA)	
	The first IP address in the combined IP range. This IP range combines IPs that the user specified in the report template (USER_IP_LIST) as well as IPs that make up the asset groups that the user specified in the report template (USER_ASSET_GROUPS).
/ASSET_DATA_REPORT/HEADER/TARGET/COMBINED_IP_LIST/RANGE/END (#PCDATA)	
	The last IP address in the combined IP range. This IP range combines IPs that the user specified in the report template (USER_IP_LIST) as well as IPs that make up the asset groups that the user specified in the report template (USER_ASSET_GROUPS).
/ASSET_DATA_REPORT/HEADER/TARGET/ASSET_TAG_LIST (INCLUDED_TAGS, EXCLUDED_TAGS?)	
/ASSET_DATA_REPORT/HEADER/TARGET/ASSET_TAG_LIST/INCLUDED_TAGS/ASSET_TAG (#PCDATA)	
	The list of asset tags included in the scan target. The scope “all” means hosts matching all tags; scope “any” means hosts matching at least one of the tags.
/ASSET_DATA_REPORT/HEADER/TARGET/ASSET_TAG_LIST/EXCLUDED_TAGS/ASSET_TAG (#PCDATA)	
	The list of asset tags excluded from the scan target. The scope “all” means hosts matching all tags; scope “any” means hosts matching at least one of the tags.
/ASSET_DATA_REPORT/RISK_SCORE_SUMMARY (TOTAL_VULNERABILITIES, AVG_SECURITY_RISK, BUSINESS_RISK)	
/ASSET_DATA_REPORT/RISK_SCORE_SUMMARY/TOTAL_VULNERABILITIES (#PCDATA)	
	The sum of the vulnerabilities found on all hosts in the report.
/ASSET_DATA_REPORT/RISK_SCORE_SUMMARY/AVG_SECURITY_RISK (#PCDATA)	
	The average security risk calculated for the report.
/ASSET_DATA_REPORT/RISK_SCORE_SUMMARY/RISK, BUSINESS_RISK (#PCDATA)	
	The business risk score calculated for the report.

Security Risk Score per Host

XPath	element specifications / notes
/ASSET_DATA_REPORT/RISK_SCORE_PER_HOST (HOSTS+)	
/ASSET_DATA_REPORT/RISK_SCORE_PER_HOST/HOSTS	(IP_ADDRESS, NETWORK?, TOTAL_VULNERABILITIES, SECURITY_RISK)
/ASSET_DATA_REPORT/RISK_SCORE_PER_HOST/HOSTS/IP_ADDRESS (#PCDATA)	The IP address of a host.
/ASSET_DATA_REPORT/RISK_SCORE_PER_HOST/HOSTS/NETWORK (#PCDATA)	The name of the network the host belongs to, when network support is enabled.
/ASSET_DATA_REPORT/RISK_SCORE_PER_HOST/HOSTS/TOTAL_VULNERABILITIES (#PCDATA)	The total number of vulnerabilties found on the host.
/ASSET_DATA_REPORT/RISK_SCORE_PER_HOST/HOSTS/SECURITY_RISK (#PCDATA)	The security risk score, either the average severity level detected or the highest severity level detected, based on the security risk setup setting for the subscription. For Express Lite, the average severity level is used.

Host List

The host list section includes a list of hosts in your report with detected vulnerabilities. For each vulnerability, information specific to its detection on the host is also included.

XPath	element specifications / notes
/ASSET_DATA_REPORT/HOST_LIST (HOST+)	
/ASSET_DATA_REPORT/HOST_LIST/HOST	(ERROR | (IP, NETWORK?, TRACKING_METHOD, ASSET_TAGS?, DNS?, NETBIOS?, OPERATING_SYSTEM?, OS_CPE?, ASSET_GROUPS?, VULN_INFO_LIST?))
/ASSET_DATA_REPORT/HOST_LIST/HOST/IP (#PCDATA)	The IP address of a host.
/ASSET_DATA_REPORT/HOST_LIST/HOST/NETWORK (#PCDATA)	The network the host belongs to, when network support is enabled.
/ASSET_DATA_REPORT/HOST_LIST/HOST/TRACKING_METHOD (#PCDATA)	The tracking method. A valid value is “IP”, “DNS”, or “NETBIOS”.
/ASSET_DATA_REPORT/HOST_LIST/HOST/ASSET_TAGS (ASSET_TAG+)	
/ASSET_DATA_REPORT/HOST_LIST/HOST/ASSET_TAGS/ASSET_TAG (#PCDATA)	An asset tag assigned to the host.
/ASSET_DATA_REPORT/HOST_LIST/HOST/DNS (#PCDATA)	The DNS host name when known.
/ASSET_DATA_REPORT/HOST_LIST/HOST/NETBIOS (#PCDATA)	The Microsoft Windows NetBIOS host name if appropriate, when known.

XPath	element specifications / notes
/ASSET_DATA_REPORT/HOST_LIST/HOST/OPERATING_SYSTEM (#PCDATA)	
	The operating system detected on the host.
/ASSET_DATA_REPORT/HOST_LIST/HOST/OS_CPE (#PCDATA)	
	The OS CPE name assigned to the operating system detected on the host. (The OS CPE name appears only when the OS CPE feature is enabled for the subscription, and an authenticated scan was run on this host after enabling this feature.)
/ASSET_DATA_REPORT/HOST_LIST/HOST/ASSET_GROUPS (ASSET_GROUP_TITLE+)	
/ASSET_DATA_REPORT/HOST_LIST/HOST/ASSET_GROUPS/ASSET_GROUP_TITLE (#PCDATA)	
	The title of an asset group that the host belongs to. This list includes all asset groups that the host belongs to in the user's account.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST (VULN_INFO+)	
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO	
	(QID, TYPE, PORT?, SERVICE?, FQDN?, PROTOCOL?, SSL?, INSTANCE?, RESULT?, FIRST_FOUND?, LAST_FOUND?, TIMES_FOUND?, VULN_STATUS?, CVSS_FINAL?, TICKET_NUMBER?, TICKET_STATE?)
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/QID (#PCDATA)	
	The Qualys ID (QID) assigned to the vulnerability.
attribute: **id**	**id** is *required* and is a reference ID that corresponds to a QID defined under the Glossary section. For more information, see /ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/QID
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/TYPE (#PCDATA)	
	The type of vulnerability check. A valid value is "Vuln" for a confirmed vulnerability, "Practice" for a potential vulnerability, or "Ig" for an information gathered.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/PORT (#PCDATA)	
	The port number that the vulnerability was detected on.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/SERVICE (#PCDATA)	
	The service that the vulnerability was detected on.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/FQDN (#PCDATA)	
	The Fully Qualified Domain Name (FQDN) associated with the host.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/PROTOCOL (#PCDATA)	
	The protocol that the vulnerability was detected on.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/SSL (#PCDATA)	
	A flag indicating whether SSL was present on this host. If SSL was present, the SSL element appears with the value "true".
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/RESULT (#PCDATA)	
	Specific scan test results for the vulnerability, from the host assessment data.
attribute: **format**	**format** is *implied* and, if present, will be "table," indicating that the results are a table that has columns separated by tabulation characters and rows separated by new-line characters

XPath	element specifications / notes
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/FIRST_FOUND (#PCDATA)	
	The date and time when the vulnerability was first detected on the host, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/LAST_FOUND (#PCDATA)	
	The date and time when the vulnerability was last detected on the host (from the most recent scan), in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/TIMES_FOUND (#PCDATA)	
	The total number of times the vulnerability was detected on the host.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/VULN_STATUS (#PCDATA)	
	The vulnerability status. (Note that status levels do not apply to information gathered.) A valid value is "New" for an active vulnerability that was detected one time, Active for an active vulnerability that was detected at least two times, "Re-Opened" for an active vulnerability that was fixed and then re-opened, and "Fixed" for a vulnerability that was detected previously and is now fixed.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/CVSS_FINAL (#PCDATA)	
	The final CVSS score calculated for the host.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/TICKET_NUMBER (#PCDATA)	
	The number of the ticket that applies to the vulnerability instance on the host.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/TICKET_STATE (#PCDATA)	
	The state/status of the ticket that applies to the vulnerability instance on the host.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/INSTANCE (#PCDATA)	
	The Oracle DB instance the vulnerability was detected on.
/ASSET_DATA_REPORT/HOST_LIST/HOST/ERROR (#PCDATA)	
attribute: **number**	**number** is *implied* and, if present, will be an error code.

Glossary

The glossary section includes static vulnerability details.

XPath	element specifications / notes
/ASSET_DATA_REPORT/GLOSSARY (VULN_DETAILS_LIST)	
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST (VULN_DETAILS+)	
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS	
	(QID, TITLE, SEVERITY, CATEGORY, CUSTOMIZED?, THREAT, THREAT_COMMENT?, IMPACT, IMPACT_COMMENT?, SOLUTION, SOLUTION_COMMENT?, COMPLIANCE?, CORRELATION?, PCI_FLAG, LAST_UPDATE?, CVSS_SCORE?, VENDOR_REFERENCE_LIST?, CVE_ID_LIST?, BUGTRAQ_ID_LIST?)

XPath	element specifications / notes
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/QID (#PCDATA)	
	The Qualys ID (QID) assigned to the vulnerability.
attribute: **id**	**id** is *required* and is a reference ID that corresponds to a QID listed in the Host List section. For more information, see /ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/QID
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/TITLE (#PCDATA)	
	The title of the vulnerability.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/SEVERITY (#PCDATA)	
	The severity level assigned to the vulnerability.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CATEGORY (#PCDATA)	
	The category of the vulnerability.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CUSTOMIZED	
	(DISABLED?, CUSTOM_SEVERITY?)
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CUSTOMIZED/DISABLED	
	(#PCDATA)
	Identifies whether the vulnerability was disabled by a Manager users. If disabled, the vulnerabilities is filtered from reports.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CUSTOMIZED/ CUSTOM_SEVERITY (#PCDATA)	
	Identifies whether the severity level was changed. Managers can change the severity level by editing the vulnerability in the Qualys KnowledgeBase.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/THREAT (#PCDATA)	
	The Qualys provided description of the threat.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/THREAT_COMMENT (#PCDATA)	
	User-defined description of the threat, if any.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/IMPACT (#PCDATA)	
	The Qualys provided description of the impact.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/IMPACT_COMMENT (#PCDATA)	
	User-defined description of the impact, if any.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/ SOLUTION (#PCDATA)	
	The Qualys provided description of the solution. When virtual patch information is correlated with a vulnerability, the virtual patch information from Trend Micro appears under the heading “Virtual Patches:”. This includes a list of virtual patches and a link to more information.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/ SOLUTION_COMMENT (#PCDATA)	
	User-defined description of the solution, if any.

XPath	element specifications / notes
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/PCI_FLAG (#PCDATA)	
	A flag that indicates whether the vulnerability must be fixed to pass a PCI compliance scan. The value "1" indicates the vulnerability must be fixed to pass PCI compliance. The value "0" indicates the vulnerability does not need to be fixed to pass PCI compliance.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION	(EXPLOITABILITY?, MALWARE?)
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/EXPLOITABILITY (EXPLT_SRC)+	
	The <EXPLOITABILITY> element and its sub-elements appear only when there is exploitability information for the vulnerability from third party vendors and/or publicly available sources.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC (SRC_NAME, EXPLT_LIST)	
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/SRC_NAME (#PCDATA)	
	The name of a third party vendor or publicly available source of the vulnerability information.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST (EXPLT)+	
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT (REF, DESC, LINK?)	
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/REF (#PCDATA)	
	The CVE reference for the exploitability information.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/DESC (#PCDATA)	
	The description provided by the source of the exploitability information (third party vendor or publicly available source).
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/LINK (#PCDATA)	
	A link to the exploit, when available.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/MALWARE (MW_SRC)+	
	The <MALWARE> element and its sub-elements appear only when there is malware information for the vulnerability from Trend Micro.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/MALWARE/MW_SRC (SRC_NAME, MW_LIST)	
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/MALWARE/MW_SRC/SRC_NAME (#PCDATA)	
	The name of the source of the malware information: Trend Micro.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST (MW_INFO)+	

XPath	element specifications / notes
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO	(MW_ID, MW_TYPE?, MW_PLATFORM?, MW_ALIAS?, MW_RATING?, MW_LINK?)
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_ID (#PCDATA)	The malware name/ID assigned by Trend Micro.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_TYPE (#PCDATA)	The type of malware, such as Backdoor, Virus, Worm or Trojan.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_PLATFORM (#PCDATA)	A list of the platforms that may be affected by the malware.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_ALIAS (#PCDATA)	A list of other names used by different vendors and/or publicly available sources to refer to the same threat.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_RATING (#PCDATA)	The overall risk rating as determined by Trend Micro: Low, Medium or High.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_LINK (#PCDATA)	A link to malware details.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/LAST_UPDATE (#PCDATA)	The date and time when the vulnerability was last updated in the Qualys KnowledgeBase, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CVSS_SCORE	(CVSS_BASE?, CVSS_TEMPORAL?)
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CVSS_SCORE/CVSS_BASE	(#PCDATA)
	The CVSS Base score defined for the vulnerability.
attribute: **source**	Note: This attribute is never present in XML output for this release.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CVSS_SCORE/CVSS_TEMPORAL	(#PCDATA)
	The CVSS Temporal score defined for the vulnerability.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/VENDOR_REFERENCE_LIST	(VENDOR_REFERENCE+)
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/VENDOR_REFERENCE_LIST/VENDOR_REFERENCE (ID, URL)	The name of a vendor reference, and the URL to this vendor reference.

XPath	element specifications / notes
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/reference_list/reference/ID	
	(#PCDATA)
	The name of a vendor reference, CVE name, or Bugtraq ID.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/reference_list/reference/URL	
	(#PCDATA)
	The URL to the vendor reference, CVE name, or Bugtraq ID.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CVE_ID_LIST (CVE_ID+)	
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CVE_ID_LIST/CVE_ID (ID, URL)	
	A CVE name assigned to the vulnerability, and the URL to this CVE name. CVE (Common Vulnerabilities and Exposures) is a list of common names for publicly known vulnerabilities and exposures. Through open and collaborative discussions, the CVE Editorial Board determines which vulnerabilities or exposures are included in CVE. If the CVE name starts with CAN (candidate) then it is under consideration for entry into CVE.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/BUGTRAQ_ID_LIST	
	(BUGTRAQ_ID+)
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/BUGTRAQ_ID_LIST/BUGTRAQ_ID	
	(ID, URL)
	A Bugtraq ID assigned to the vulnerability, and the URL to this Bugtraq ID.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/COMPLIANCE	
	(COMPLIANCE_INFO+)
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/COMPLIANCE/ COMPLIANCE_INFO (COMPLIANCE_TYPE, COMPLIANCE_SECTION, COMPLIANCE_DESCRIPTION)	
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/COMPLIANCE/ COMPLIANCE_INFO/COMPLIANCE_TYPE (#PCDATA)	
	The type of a compliance policy or regulation that is associated with the vulnerability. A valid value is: HIPAA, GLBA, CobIT or SOX.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/COMPLIANCE/ COMPLIANCE_INFO/COMPLIANCE_SECTION (#PCDATA)	
	The section of a compliance policy or regulation associated with the vulnerability.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/COMPLIANCE/ COMPLIANCE_INFO/COMPLIANCE_DESCRIPTION (#PCDATA)	
	The description of a compliance policy or regulation associated with the vulnerability.

Appendices

The appendices section includes additional report information including hosts for which there are no scan results and report template settings.

XPath	element specifications / notes
/ASSET_DATA_REPORT/APPENDICES	(NO_RESULTS?, NO_VULNS?, TEMPLATE_DETAILS?)
/ASSET_DATA_REPORT/APPENDICES/NO_RESULTS	(IP_LIST)
	A list of IPs for which there are no available scan results. This includes hosts that were not "alive" at the time of the scan.
/ASSET_DATA_REPORT/APPENDICES/NO_RESULTS /IP_LIST	(NETWORK?, RANGE*)
/ASSET_DATA_REPORT/APPENDICES/NO_RESULTS /IP_LIST/NETWORK	(#PCDATA)
	The network the IPs belong to, when network support is enabled.
/ASSET_DATA_REPORT/APPENDICES/NO_RESULTS/IP_LIST/RANGE	(START, END)
/ASSET_DATA_REPORT/APPENDICES/NO_RESULTS/IP_LIST/RANGE/START	(#PCDATA)
	The first IP address in the range.
/ASSET_DATA_REPORT/APPENDICES/NO_RESULTS/IP_LIST/RANGE/END	(#PCDATA)
	The last IP address in the range.
/ASSET_DATA_REPORT/APPENDICES/NO_VULNS	(IP_LIST)
	A list of IPs for which you have saved scan results but the results are not displayed because all vulnerability checks have been filtered out. To display these results, make changes to the filter settings in your report template. This appendix also lists IPs for which no vulnerabilities were detected by the service. Verify the scan options specified in your option profile.
/ASSET_DATA_REPORT/APPENDICES/NO_VULNS/IP_LIST	(NETWORK?, RANGE*)
/ASSET_DATA_REPORT/APPENDICES/NO_VULNS/IP_LIST/NETWORK	(#PCDATA)
	The network the IPs belong to, when network support is enabled.
/ASSET_DATA_REPORT/APPENDICES/NO_VULNS/IP_LIST/RANGE	(START, END)
/ASSET_DATA_REPORT/APPENDICES/NO_VULNS/IP_LIST/RANGE/START	(#PCDATA)
	The first IP address in the range.
/ASSET_DATA_REPORT/APPENDICES/NO_VULNS/IP_LIST/RANGE/END	(#PCDATA)
	The last IP address in the range.
/ASSET_DATA_REPORT/APPENDICES/TEMPLATE_DETAILS	(VULN_LISTS?, SELECTIVE_VULNS?, EXCLUDED_VULN_LISTS?, EXCLUDED_VULNS?, RESULTING_VULNS?, FILTER_SUMMARY?, EXCLUDED_CATEGORIES?)
/ASSET_DATA_REPORT/APPENDICES/TEMPLATE_DETAILS/VULN_LISTS	(#PCDATA)
	The title of each included search list when specified in the report template.
/ASSET_DATA_REPORT/APPENDICES/TEMPLATE_DETAILS/SELECTIVE_VULNS	(#PCDATA)
/ASSET_DATA_REPORT/APPENDICES/TEMPLATE_DETAILS/EXCLUDED_VULN_LISTS	(#PCDATA)
	The title of each excluded search list when specified in the report template.

XPath	element specifications / notes
/ASSET_DATA_REPORT/APPENDICES/TEMPLATE_DETAILS/EXCLUDED_VULNS (#PCDATA)	
	All excluded QIDs contained in the excluded search lists specified in the report template.
/ASSET_DATA_REPORT/APPENDICES/TEMPLATE_DETAILS/RESULTING_VULNS (#PCDATA)	
	This element appears when both included search lists and excluded search lists were specified in the report template. When present, this element contains the resulting list of included QIDs, where all excluded QIDs have been removed. No value appears if there were no resulting QIDs.
/ASSET_DATA_REPORT/APPENDICES/TEMPLATE_DETAILS/FILTER_SUMMARY (#PCDATA)	
	A summary of the filters set on the Filter tab in the report template. For example, you may filter particular status levels, severity levels and types of vulnerability checks (active, disabled and ignored) for vulnerabilities, potential vulnerabilities and information gathered.
/ASSET_DATA_REPORT/APPENDICES/TEMPLATE_DETAILS/EXCLUDED_CATEGORIES (#PCDATA)	
	A list of vulnerability categories that were filtered out of the report. Identify which vulnerability categories to include on the Filter tab in the report template.

APPENDIX E

Remediation Management Reports

The remediation management reports provide information about hosts and remediation tickets in the API user's account. These reports are returned from the functions described in Chapter 6.

This appendix describes these reports:

- Ticket List Output
- Ticket Edit Output
- Ticket Delete Output
- Deleted Ticket List
- Get Ticket Information Report
- Get Host Information Report
- Ignore Vulnerability Output

Ticket List Output

The ticket list output (ticket_list_output.dtd) is an XML report returned from the **`ticket_list.php`** function. This report includes information on selected tickets.

DTD for Ticket List Output

A recent DTD for the remediation ticket list output (ticket_list_output.dtd) is shown below.

```
<!-- QUALYS TICKET LIST OUTPUT DTD -->

<!ELEMENT REMEDIATION_TICKETS (ERROR | (HEADER,  (TICKET_LIST,
                               TRUNCATION?)?))>

<!-- Ticket Report error -->
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!-- Truncation warning -->
<!ELEMENT TRUNCATION (#PCDATA)>
<!ATTLIST TRUNCATION last CDATA #IMPLIED>

<!-- Information about the Ticket Report -->
<!ELEMENT HEADER (USER_LOGIN, COMPANY, DATETIME, WHERE)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT COMPANY (#PCDATA)>
<!ELEMENT DATETIME (#PCDATA)>

<!-- Search criteria -->
<!ELEMENT WHERE ((MODIFIED_SINCE_DATETIME?,UNMODIFIED_SINCE_DATETIME?,
                  TICKET_NUMBERS?, SINCE_TICKET_NUMBER?,
                  UNTIL_TICKET_NUMBER?, STATES?, IPS?, ASSET_GROUPS?,
                  DNS_CONTAINS?, NETBIOS_CONTAINS?, VULN_SEVERITIES?,
                  POTENTIAL_VULN_SEVERITIES?, OVERDUE?, INVALID?,
                  TICKET_ASSIGNEE?, QIDS?, SHOW_VULN_DETAILS?,
                  VULN_TITLE_CONTAINS?, VULN_DETAILS_CONTAINS?,
                  VENDOR_REF_CONTAINS?)+) >
<!ELEMENT MODIFIED_SINCE_DATETIME (#PCDATA)>
<!ELEMENT UNMODIFIED_SINCE_DATETIME (#PCDATA)>
<!ELEMENT TICKET_NUMBERS (#PCDATA)>
<!ELEMENT SINCE_TICKET_NUMBER (#PCDATA)>
<!ELEMENT UNTIL_TICKET_NUMBER (#PCDATA)>
<!ELEMENT STATES (#PCDATA)>
<!ELEMENT IPS (#PCDATA)>
<!ELEMENT ASSET_GROUPS (#PCDATA)>
<!ELEMENT DNS_CONTAINS (#PCDATA)>
<!ELEMENT NETBIOS_CONTAINS (#PCDATA)>
```

```
<!ELEMENT VULN_SEVERITIES (#PCDATA)>
<!ELEMENT POTENTIAL_VULN_SEVERITIES (#PCDATA)>
<!ELEMENT OVERDUE (#PCDATA)>
<!ELEMENT INVALID (#PCDATA)>
<!ELEMENT TICKET_ASSIGNEE (#PCDATA)>
<!ELEMENT QIDS (#PCDATA)>
<!ELEMENT SHOW_VULN_DETAILS (#PCDATA)>
<!ELEMENT VULN_TITLE_CONTAINS (#PCDATA)>
<!ELEMENT VULN_DETAILS_CONTAINS (#PCDATA)>
<!ELEMENT VENDOR_REF_CONTAINS (#PCDATA)>

<!-- AVOID COLISIONS BETWEEN LISTS ABOVE AND BELOW!-->
<!ELEMENT TICKET_LIST (TICKET+)>
<!ELEMENT TICKET (NUMBER, CREATION_DATETIME, DUE_DATETIME,
                  CURRENT_STATE, CURRENT_STATUS?, INVALID?, ASSIGNEE,
                  DETECTION, STATS?, HISTORY_LIST?, VULNINFO?, DETAILS?)>
<!ELEMENT NUMBER (#PCDATA)>
<!ELEMENT CREATION_DATETIME (#PCDATA)>
<!ELEMENT DUE_DATETIME (#PCDATA)>
<!ELEMENT CURRENT_STATE (#PCDATA)>
<!ELEMENT CURRENT_STATUS (#PCDATA)>
<!ELEMENT ASSIGNEE (NAME, EMAIL, LOGIN)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT EMAIL (#PCDATA)>
<!ELEMENT LOGIN (#PCDATA)>

<!-- Target Asset -->
<!ELEMENT DETECTION (IP, DNSNAME?, NBHNAME?, PORT?, SERVICE?, PROTOCOL?,
                     FQDN?, SSL?, INSTANCE?)>
<!ELEMENT IP (#PCDATA) >
<!-- DNS Hostname -->
<!ELEMENT DNSNAME (#PCDATA)>
<!-- NetBios Hostname -->
<!ELEMENT NBHNAME (#PCDATA)>
<!-- TCP Port of the vuln -->
<!ELEMENT PORT (#PCDATA)>
<!-- service name on the host-->
<!ELEMENT SERVICE (#PCDATA)>
<!-- Protocol -->
<!ELEMENT PROTOCOL (#PCDATA)>
<!-- FQDN -->
<!ELEMENT FQDN (#PCDATA)>
<!-- was this found using SSL -->
<!ELEMENT SSL (#PCDATA)>
<!-- Ticket Statistics -->
<!ELEMENT INSTANCE (#PCDATA)>
<!ELEMENT STATS (FIRST_FOUND_DATETIME, LAST_FOUND_DATETIME,
                 LAST_SCAN_DATETIME, TIMES_FOUND, TIMES_NOT_FOUND,
                 LAST_OPEN_DATETIME, LAST_RESOLVED_DATETIME?,
```

```
                  LAST_CLOSED_DATETIME?, LAST_IGNORED_DATETIME?)>
<!ELEMENT FIRST_FOUND_DATETIME (#PCDATA)>
<!ELEMENT LAST_FOUND_DATETIME (#PCDATA)>
<!ELEMENT LAST_SCAN_DATETIME (#PCDATA)>
<!ELEMENT TIMES_FOUND (#PCDATA)>
<!ELEMENT TIMES_NOT_FOUND (#PCDATA)>
<!ELEMENT LAST_OPEN_DATETIME (#PCDATA)>
<!ELEMENT LAST_RESOLVED_DATETIME (#PCDATA)>
<!ELEMENT LAST_CLOSED_DATETIME (#PCDATA)>
<!ELEMENT LAST_IGNORED_DATETIME (#PCDATA)>

<!-- Ticket History -->
<!ELEMENT HISTORY_LIST (HISTORY+)>
<!ELEMENT HISTORY (DATETIME, ACTOR,
                   STATE?, ADDED_ASSIGNEE?, REMOVED_ASSIGNEE?,
                   SCAN?, RULE?, COMMENT?) >
<!ELEMENT ACTOR (#PCDATA)>

<!-- Ticket state/status -->
<!ELEMENT STATE (OLD?, NEW)>
<!ELEMENT OLD (#PCDATA)>
<!ELEMENT NEW (#PCDATA)>

<!-- added assignee -->
<!ELEMENT ADDED_ASSIGNEE (NAME, EMAIL, LOGIN)>

<!-- removed assignee -->
<!ELEMENT REMOVED_ASSIGNEE (NAME, EMAIL, LOGIN)>

<!-- Scan Report that triggered ticket policy -->
<!ELEMENT SCAN (REF, DATETIME?)>
<!ELEMENT REF (#PCDATA)>

<!-- Ticket Creation Rule (Policy) -->
<!ELEMENT RULE (#PCDATA) >

<!-- Ticket Comment -->
<!ELEMENT COMMENT (#PCDATA) >
<!-- Ticket Vulnerability Information -->
<!ELEMENT VULNINFO (TITLE, TYPE, QID, SEVERITY, STANDARD_SEVERITY,
                    CVE_ID_LIST?, VENDOR_REF_LIST?)>
<!--
    Severity is Qualys severity level 1 to 5 (possibly customized),
    whereas standard-severity is the original Qualys severity level
    1 to 5 (which may differ if the vuln has been customized by one
    of the users in the subscription).
-->
<!ELEMENT TITLE (#PCDATA)>
<!-- VULN|POSS -->
```

```
<!ELEMENT TYPE (#PCDATA)>
<!ELEMENT QID (#PCDATA)>
<!ELEMENT SEVERITY (#PCDATA)>
<!ELEMENT STANDARD_SEVERITY (#PCDATA)>

<!-- CVE ID (no URI) -->
<!ELEMENT CVE_ID_LIST (CVE_ID+)>
<!ELEMENT CVE_ID (#PCDATA) >
<!-- Vendor Reference (no URI) -->
<!ELEMENT VENDOR_REF_LIST (VENDOR_REF+)>
<!ELEMENT VENDOR_REF (#PCDATA) >

<!-- Ticket Vulnerability Details -->
<!ELEMENT DETAILS
(DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,CORRELATION?,RESULT?)>
<!ELEMENT DIAGNOSIS (#PCDATA) >
<!ELEMENT CONSEQUENCE (#PCDATA) >
<!ELEMENT SOLUTION (#PCDATA) >

<!ELEMENT CORRELATION (EXPLOITABILITY?,MALWARE?)>
<!ELEMENT EXPLOITABILITY (EXPLT_SRC)+>
<!ELEMENT EXPLT_SRC (SRC_NAME, EXPLT_LIST)>
<!ELEMENT SRC_NAME (#PCDATA)>
<!ELEMENT EXPLT_LIST (EXPLT)+>
<!ELEMENT EXPLT (REF, DESC, LINK?)>
<!ELEMENT DESC (#PCDATA)>
<!ELEMENT LINK (#PCDATA)>

<!ELEMENT MALWARE (MW_SRC)+>
<!ELEMENT MW_SRC (SRC_NAME, MW_LIST)>
<!ELEMENT MW_LIST (MW_INFO)+>
<!ELEMENT MW_INFO (MW_ID, MW_TYPE?, MW_PLATFORM?, MW_ALIAS?, MW_RATING?,
                   MW_LINK?)>
<!ELEMENT MW_ID (#PCDATA)>
<!ELEMENT MW_TYPE (#PCDATA)>
<!ELEMENT MW_PLATFORM (#PCDATA)>
<!ELEMENT MW_ALIAS (#PCDATA)>
<!ELEMENT MW_RATING (#PCDATA)>
<!ELEMENT MW_LINK (#PCDATA)>
<!ELEMENT RESULT (#PCDATA) >

<!--
    If the "format" attribute is set to "table", then column
    values are separated by tab '\t', and rows are terminated
    by new line '\n'.
-->
<!ATTLIST RESULT format CDATA #IMPLIED>
```

XPaths for Ticket List Output

This section describes the XPaths for the ticket list output (ticket_list_output.dtd).

Ticket List — Header Information

XPath	element specifications / notes
/REMEDIATION_TICKETS	(ERROR | (HEADER, (TICKET_LIST, TRUNCATION?)?))
/REMEDIATION_TICKETS/ERROR (#PCDATA)	
attribute: **number**	**number** is *implied* and if present, is an error code
/REMEDIATION_TICKETS/TRUNCATION (#PCDATA)	
attribute: **last**	**last** is *implied* and if present, is the last ticket number included in the ticket list report. The ticket list is truncated after 1000 records.
/REMEDIATION_TICKETS/HEADER (USER_LOGIN, COMPANY, DATETIME, WHERE)	
/REMEDIATION_TICKETS/HEADER/USER_LOGIN (#PCDATA)	
	The Qualys user login name for the user that requested the ticket list report.
/REMEDIATION_TICKETS/HEADER/COMPANY (#PCDATA)	
	The company associated with the Qualys user.
/REMEDIATION_TICKETS/HEADER/DATETIME (#PCDATA)	
	The date and time when the ticket list report was requested. The date appears in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT) like this: "2005-01-10T02:33:11Z".
/REMEDIATION_TICKETS/HEADER/WHERE	
	((MODIFIED_SINCE_DATETIME?,UNMODIFIED_SINCE_DATETIME?, TICKET_NUMBERS?, SINCE_TICKET_NUMBER?, UNTIL_TICKET_NUMBER?, STATES?, IPS?, ASSET_GROUPS?, DNS_CONTAINS?, NETBIOS_CONTAINS?, VULN_SEVERITIES?, POTENTIAL_VULN_SEVERITIES?, OVERDUE?, INVALID?, TICKET_ASSIGNEE?, QIDS?, SHOW_VULN_DETAILS?, VULN_TITLE_CONTAINS?, VULN_DETAILS_CONTAINS?, VENDOR_REF_CONTAINS?) +)
	Ticket selection parameters that were specified as part of the ticket_list.php request. Only the specified parameters appear in the output. Ticket selection parameters are described below.
/REMEDIATION_TICKETS/HEADER/WHERE/MODIFIED_SINCE_DATETIME (#PCDATA)	
	The start date/time of a time window when tickets were modified. The end of the time window is the date/time when the API function was run. Only tickets modified within this time window are retrieved. The start date/time appears in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT) like "2006-01-01" or "2006-05-25T23:12:00Z".

XPath	element specifications / notes
/REMEDIATION_TICKETS/HEADER/WHERE/UNMODIFIED_SINCE_DATETIME (#PCDATA)	
	The start date/time of the time window when tickets were not modified. The end of the time window is the date/time when the API function was run. Only tickets that were not modified within this time window are retrieved. The start date/time appears in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT) like "2006-01-01" or "2006-05-25T23:12:00Z".
/REMEDIATION_TICKETS/HEADER/WHERE/TICKET_NUMBERS (#PCDATA)	
	One or more ticket numbers and/or ranges. Ticket range start and end is separated by a dash (-).
/REMEDIATION_TICKETS/HEADER/WHERE/SINCE_TICKET_NUMBER (#PCDATA)	
	The lowest ticket number selected. Selected tickets will have numbers greater than or equal to the ticket number specified.
/REMEDIATION_TICKETS/HEADER/WHERE/UNTIL_TICKET_NUMBER (#PCDATA)	
	The highest ticket number selected. Selected tickets will have numbers less than or equal to the ticket number specified.
/REMEDIATION_TICKETS/HEADER/WHERE/STATES (#PCDATA)	
	One or more ticket states. Possible values are OPEN (for state/status Open or Open/Reopened), RESOLVED (for state Resolved), CLOSED (for state/status Closed/Fixed) and IGNORED (for state/status Closed/Ignored).
/REMEDIATION_TICKETS/HEADER/WHERE/IPS (#PCDATA)	
	One or more IP addresses and/or ranges.
/REMEDIATION_TICKETS/HEADER/WHERE/ASSET_GROUPS (#PCDATA)	
	The title of one or more asset groups.
/REMEDIATION_TICKETS/HEADER/WHERE/DNS_CONTAINS (#PCDATA)	
	A text string contained within the DNS host name.
/REMEDIATION_TICKETS/HEADER/WHERE/NETBIOS_CONTAINS (#PCDATA)	
	A text string contained within the NetBIOS host name.
/REMEDIATION_TICKETS/HEADER/WHERE/VULN_SEVERITIES (#PCDATA)	
	One or more vulnerability severity levels.
/REMEDIATION_TICKETS/HEADER/WHERE/POTENTIAL_VULN_SEVERITIES (#PCDATA)	
	One or more potential vulnerability severity levels.
/REMEDIATION_TICKETS/HEADER/WHERE/OVERDUE (#PCDATA)	
	When not specified, overdue and non-overdue tickets are selected. The value 1 indicates that only overdue tickets were requested. The value 0 indicates that only non-overdue tickets were requested.
/REMEDIATION_TICKETS/HEADER/WHERE/INVALID (#PCDATA)	
	When not specified, both valid and invalid tickets are selected. The value 1 indicates that only invalid tickets were requested. The value 0 indicates that only valid tickets that were requested.

XPath	element specifications / notes
/REMEDIATION_TICKETS/HEADER/WHERE/TICKET_ASSIGNEE (#PCDATA)	
	The user login of an active account.
/REMEDIATION_TICKETS/HEADER/WHERE/QIDS (#PCDATA)	
	One or more Qualys IDs (QIDs).
/REMEDIATION_TICKETS/HEADER/WHERE/SHOW_VULN_DETAILS (#PCDATA)	
	A flag identifying whether vulnerability details are included in the ticket list XML output. The value 1 indicates that vulnerability details were requested. The value 0 indicates that vulnerability details were not requested.
/REMEDIATION_TICKETS/HEADER/WHERE/VULN_TITLE_CONTAINS (#PCDATA)	
	A text string contained within the vulnerability title.
/REMEDIATION_TICKETS/HEADER/WHERE/VULN_DETAILS_CONTAINS (#PCDATA)	
	A text string contained within vulnerability details.
/REMEDIATION_TICKETS/HEADER/WHERE/VENDOR_REF_CONTAINS (#PCDATA)	
	A text string contained within a vendor reference for the vulnerability.

Ticket List — General Ticket Information

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET_LIST (TICKET+)	
/REMEDIATION_TICKETS/TICKET_LIST/TICKET	
	(NUMBER, CREATION_DATETIME, DUE_DATETIME, CURRENT_STATE, CURRENT_STATUS?, INVALID?, ASSIGNEE, DETECTION, STATS?, HISTORY_LIST?, VULNINFO?, DETAILS?)
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/NUMBER (#PCDATA)	
	The number assigned to the ticket by Qualys.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/CREATION_DATETIME (#PCDATA)	
	The date when the ticket was first created in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DUE_DATETIME (#PCDATA)	
	The due date for ticket resolution in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/CURRENT_STATE (#PCDATA)	
	The current ticket state: OPEN, RESOLVED, or CLOSED.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/CURRENT_STATUS (#PCDATA)	
	The current ticket status: REOPENED, FIXED, IGNORED.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/INVALID (#PCDATA)	
	A flag indicating whether the ticket is currently invalid. The value 1 is returned when the ticket is invalid. The value 0 is returned when the ticket is valid.

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/ASSIGNEE	(NAME, EMAIL, LOGIN)
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/ASSIGNEE/NAME	(#PCDATA)
	The full name (first and last) of the assignee, as defined in the assignee's Qualys user account.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/ASSIGNEE/EMAIL	(#PCDATA)
	The email address of the assignee, as defined in the assignee's Qualys user account.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/ASSIGNEE/LOGIN	(#PCDATA)
	The Qualys user login name for the assignee.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETECTION	(#PCDATA)
	See "Ticket List — Host Information" for descriptions of the DETECTION sub-elements.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/STATS	(#PCDATA)
	See "Ticket List — Statistics" for descriptions of the STATS sub-elements.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST	(#PCDATA)
	See "Ticket List — History" for descriptions of the HISTORY sub-elements.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/VULNINFO	(#PCDATA)
	See "Ticket List — Vulnerability Information" for descriptions of the VULNINFO sub-elements.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS	(#PCDATA)
	See "Ticket List — Vulnerability Details" for descriptions of the DETAILS sub-elements.

Ticket List — Host Information

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETECTION	(IP, DNSNAME?, NBHNAME?, PORT?, SERVICE?, PROTOCOL?, FQDN?, SSL?, INSTANCE?)
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETECTION/IP	(#PCDATA)
	The IP address of the host.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETECTION/DNSNAME	(#PCDATA)
	The DNS host name when known.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETECTION/NBHNAME	(#PCDATA)
	The Microsoft Windows NetBIOS host name if appropriate, when known.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETECTION/PORT	(#PCDATA)
	The port number that the vulnerability was detected on.

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETECTION/SERVICE (#PCDATA)	
	The service that the vulnerability was detected on.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETECTION/PROTOCOL (#PCDATA)	
	The protocol that the vulnerability was detected on.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETECTION/FQDN (#PCDATA)	
	The fully qualified domain name of the host, when known.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETECTION/SSL (#PCDATA)	
	A flag indicating whether SSL was present on this host, when known. If SSL was present, the SSL element appears with the value TRUE.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETECTION/INSTANCE (#PCDATA)	
	The Oracle DB instance the vulnerability was detected on.

Ticket List — Statistics

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/STATS	
	(FIRST_FOUND_DATETIME, LAST_FOUND_DATETIME, LAST_SCAN_DATETIME, TIMES_FOUND, TIMES_NOT_FOUND, LAST_OPEN_DATETIME, LAST_RESOLVED_DATETIME?, LAST_CLOSED_DATETIME?, LAST_IGNORED_DATETIME?)
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/STATS/FIRST_FOUND_DATETIME (#PCDATA)	
	The date and time when the vulnerability was first detected on the host, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/STATS/LAST_FOUND_DATETIME (#PCDATA)	
	The date and time when the vulnerability was last detected on the host (from the most recent scan), in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/STATS/LAST_SCAN_DATETIME (#PCDATA)	
	The date and time of the most recent scan of the host, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/STATS/TIMES_FOUND (#PCDATA)	
	The total number of times the vulnerability was detected on the host.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/STATS/TIMES_NOT_FOUND (#PCDATA)	
	The total number of times the host was scanned and the vulnerability was not detected.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/STATS/LAST_OPEN_DATETIME (#PCDATA)	
	The date of the most recent scan which caused the ticket state to be changed to Open, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/STATS/LAST_RESOLVED_DATETIME (#PCDATA)	
	The date of the most recent scan which caused the ticket state to be changed to Resolved, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/STATS/LAST_CLOSED_DATETIME (#PCDATA)	
	The date of the most recent scan which caused the ticket state to be changed to Closed, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/STATS/LAST_IGNORED_DATETIME (#PCDATA)	
	The most recent date and time when the ticket was marked as Ignored, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).

Ticket List — History

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST (HISTORY+)	
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY	
	(DATETIME, ACTOR, STATE?, ADDED_ASSIGNEE?, REMOVED_ASSIGNEE?, SCAN?, RULE?, COMMENT?)
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/DATETIME (#PCDATA)	
	The date and time of the ticket history event, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/ACTOR (#PCDATA)	
	The Qualys user login name, identifying the user whose action prompted the ticket history event (such as user scan resulting in ticket state/status change, user ticket edit).
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/STATE (OLD?, NEW)	
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/STATE/OLD (#PCDATA)	
	The old (previous) state of the ticket.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/STATE/NEW (#PCDATA)	
	The new (current) state of the ticket.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/ADDED_ASSIGNEE	
	(NAME, EMAIL, LOGIN)
	Qualys user who was added as the ticket assignee. For a complete description of the ADDED_ASSIGNEE sub-elements, see the ASSIGNEE description in the "Ticket List — General Ticket Information" table.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/REMOVED_ASSIGNEE	
	(NAME, EMAIL, LOGIN)
	Qualys user who was removed as the ticket assignee. For a complete description of the REMOVED_ASSIGNEE sub-elements, see the ASSIGNEE description in the "Ticket List — General Ticket Information" table.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/SCAN (REF, DATETIME?)	
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/SCAN/REF (#PCDATA)	
	The scan report reference for the scan that triggered the ticket update event. Note: For a new ticket created by a user, a scan report reference is not returned.

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/SCAN/DATETIME (#PCDATA)	
	The date and time of the scan that triggered the ticket update event, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/RULE (#PCDATA)	
	The name of the policy rule that triggered the automatic ticket creation.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/COMMENT (#PCDATA)	
	Comments added to the ticket by Qualys users.

Ticket List — Vulnerability Information

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/VULNINFO	
	(TITLE, TYPE, QID, SEVERITY, STANDARD_SEVERITY, CVE_ID_LIST?, VENDOR_REF_LIST?)
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/VULNINFO/TITLE (#PCDATA)	
	The title of the vulnerability, from the Qualys KnowledgeBase.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/VULNINFO/TYPE (#PCDATA)	
	Type is VULN for a vulnerability, and POSS for a potential vulnerability.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/VULNINFO/QID (#PCDATA)	
	The Qualys ID (QID) assigned to the vulnerability, from the Qualys KnowledgeBase.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/VULNINFO/SEVERITY (#PCDATA)	
	The current severity level assigned to the vulnerability. This severity level may be different from the standard severity level if it was customized by a Manager user.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/VULNINFO/STANDARD_SEVERITY (#PCDATA)	
	The standard or initial severity level assigned to the vulnerability by Qualys.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/VULNINFO/CVE_ID_LIST (CVE_ID+)	
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/VULNINFO/CVE_ID_LIST/CVE_ID (#PCDATA)	
	A CVE name assigned to the vulnerability. CVE (Common Vulnerabilities and Exposures) is a list of common names for publicly known vulnerabilities and exposures. Through open and collaborative discussions, the CVE Editorial Board determines which vulnerabilities or exposures are included in CVE. If the CVE name starts with CAN (candidate) then it is under consideration for entry into CVE.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/VULNINFO/VENDOR_REF_LIST (VENDOR_REF+)	
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/VULNINFO/VENDOR_REF_LIST/VENDOR_REF	
	(#PCDATA)
	A vendor reference number assigned to the vulnerability.

Ticket List — Vulnerability Details

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS	(DIAGNOSIS?, CONSEQUENCE?, SOLUTION?, CORRELATION?, RESULT?)
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/DIAGNOSIS (#PCDATA)	A description of the threat that the vulnerability presents, from the Qualys KnowledgeBase.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CONSEQUENCES (#PCDATA)	A description of the potential impact if this vulnerability is exploited, from the Qualys KnowledgeBase.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/SOLUTION (#PCDATA)	A verified solution to fix the vulnerability, from the Qualys KnowledgeBase. When virtual patch information is correlated with a vulnerability, the virtual patch information from Trend Micro appears under the heading "Virtual Patches:". This includes a list of virtual patches and a link to more information.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION	(EXPLOITABILITY?, MALWARE?)
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/EXPLOITABILITY (EXPLT_SRC)+	The <EXPLOITABILITY> element and its sub-elements appear only when there is exploitability information for the vulnerability from third party vendors and/or publicly available sources.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC (SRC_NAME, EXPLT_LIST)	
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/SRC_NAME (#PCDATA)	The name of a third party vendor or publicly available source of the vulnerability information.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST (EXPLT)+	
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT (REF, DESC, LINK?)	
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/REF (#PCDATA)	The CVE reference for the exploitability information.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/DESC (#PCDATA)	The description provided by the source of the exploitability information (third party vendor or publicly available source).
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/LINK (#PCDATA)	A link to the exploit, when available.

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/ MALWARE (MW_SRC)+	
	The <MALWARE> element and its sub-elements appear only when there is malware information for the vulnerability from Trend Micro.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/ MALWARE/MW_SRC (SRC_NAME, MW_LIST)	
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/ MALWARE/MW_SRC/SRC_NAME (#PCDATA)	
	The name of the source of the malware information: Trend Micro.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/ MALWARE/MW_SRC/MW_LIST (MW_INFO)+	
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/ MALWARE/MW_SRC/MW_LIST/MW_INFO	
	(MW_ID, MW_TYPE?, MW_PLATFORM?, MW_ALIAS?, MW_RATING?, MW_LINK?)
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/ MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_ID (#PCDATA)	
	The malware name/ID assigned by Trend Micro.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/ MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_TYPE (#PCDATA)	
	The type of malware, such as Backdoor, Virus, Worm or Trojan.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/ MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_PLATFORM (#PCDATA)	
	A list of the platforms that may be affected by the malware.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/ MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_ALIAS (#PCDATA)	
	A list of other names used by different vendors and/or publicly available sources to refer to the same threat.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/ MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_RATING (#PCDATA)	
	The overall risk rating as determined by Trend Micro: Low, Medium or High.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/ MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_LINK (#PCDATA)	
	A link to malware details.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/RESULT (#PCDATA)	
	Specific scan test results for the vulnerability, from the host assessment data.
attribute: **format**	**format** is *implied* and if present, will be "table," indicating that the results are a table that has columns separated by tabulation characters and rows separated by new-line characters

Ticket Edit Output

The ticket edit output (ticket_edit_output.dtd) is an XML report returned from the **`ticket_edit.php`** function. This report includes a status message and identifies tickets that were changed.

DTD for Edit Ticket Output

A recent DTD for the ticket edit output (ticket_edit_output.dtd) is shown below.

```
<!-- QUALYS TICKET EDIT OUTPUT DTD -->

<!ELEMENT TICKET_EDIT_OUTPUT (ERROR | (HEADER,  CHANGES, SKIPPED))>

<!-- Ticket Report error -->
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!-- Information about the Ticket Report -->
<!ELEMENT HEADER (USER_LOGIN, COMPANY, DATETIME, UPDATE, WHERE)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT COMPANY (#PCDATA)>
<!ELEMENT DATETIME (#PCDATA)>

<!-- Edit criteria -->
<!ELEMENT UPDATE ((ASSIGNEE?, STATE?, COMMENT?, REOPEN_IGNORED_DAYS?)+) >
<!ELEMENT ASSIGNEE (#PCDATA)>
<!ELEMENT STATE (#PCDATA)>
<!ELEMENT COMMENT (#PCDATA)>
<!ELEMENT REOPEN_IGNORED_DAYS (#PCDATA)>

<!-- Search criteria -->
<!ELEMENT WHERE ((MODIFIED_SINCE_DATETIME?,UNMODIFIED_SINCE_DATETIME?,
                  TICKET_NUMBERS?, SINCE_TICKET_NUMBER?,
                  UNTIL_TICKET_NUMBER?, STATES?, IPS?, ASSET_GROUPS?,
                  DNS_CONTAINS?, NETBIOS_CONTAINS?, VULN_SEVERITIES?,
                  POTENTIAL_VULN_SEVERITIES?, OVERDUE?, INVALID?,
                  TICKET_ASSIGNEE?, QIDS?, VULN_TITLE_CONTAINS?,
                  VULN_DETAILS_CONTAINS?, VENDOR_REF_CONTAINS?)+) >
<!ELEMENT MODIFIED_SINCE_DATETIME (#PCDATA)>
<!ELEMENT UNMODIFIED_SINCE_DATETIME (#PCDATA)>
<!ELEMENT TICKET_NUMBERS (#PCDATA)>
<!ELEMENT SINCE_TICKET_NUMBER (#PCDATA)>
<!ELEMENT UNTIL_TICKET_NUMBER (#PCDATA)>
<!ELEMENT STATES (#PCDATA)>
<!ELEMENT IPS (#PCDATA)>
<!ELEMENT ASSET_GROUPS (#PCDATA)>
<!ELEMENT DNS_CONTAINS (#PCDATA)>
```

```
<!ELEMENT NETBIOS_CONTAINS (#PCDATA)>
<!ELEMENT VULN_SEVERITIES (#PCDATA)>
<!ELEMENT POTENTIAL_VULN_SEVERITIES (#PCDATA)>
<!ELEMENT OVERDUE (#PCDATA)>
<!ELEMENT INVALID (#PCDATA)>
<!ELEMENT TICKET_ASSIGNEE (#PCDATA)>
<!ELEMENT QIDS (#PCDATA)>
<!ELEMENT VULN_TITLE_CONTAINS (#PCDATA)>
<!ELEMENT VULN_DETAILS_CONTAINS (#PCDATA)>
<!ELEMENT VENDOR_REF_CONTAINS (#PCDATA)>

<!-- AVOID COLISIONS BETWEEN LISTS ABOVE AND BELOW!-->
<!ELEMENT CHANGES (TICKET_NUMBER_LIST)?>
<!ATTLIST CHANGES count CDATA #IMPLIED>

<!ELEMENT TICKET_NUMBER_LIST (TICKET_NUMBER+)>
<!ELEMENT TICKET_NUMBER (#PCDATA)>

<!ELEMENT SKIPPED (TICKET_LIST)?>
<!ATTLIST SKIPPED count CDATA #IMPLIED>

<!ELEMENT TICKET_LIST (TICKET+)>
<!ELEMENT TICKET (NUMBER, REASON)>
<!ELEMENT NUMBER (#PCDATA)>
<!ELEMENT REASON (#PCDATA)>
```

XPaths for Edit Ticket Output

This section describes the XPaths for the ticket edit output (ticket_edit_output.dtd).

Edit Ticket Output — Header Information

XPath	element specifications / notes
/TICKET_EDIT_OUTPUT	(ERROR | (HEADER, CHANGES, SKIPPED))
/TICKET_EDIT_OUTPUT/ERROR	(#PCDATA)
attribute: **number**	**number** is *implied* and, if present, is an error code.
/TICKET_EDIT_OUTPUT/HEADER	(USER_LOGIN, COMPANY, DATETIME, UPDATE, WHERE)
/TICKET_EDIT_OUTPUT/HEADER/USER_LOGIN	(#PCDATA)
	The Qualys user login name for the user that issued the ticket edit request.
/TICKET_EDIT_OUTPUT/HEADER/COMPANY	(#PCDATA)
	The company associated with the Qualys user.
/TICKET_EDIT_OUTPUT/HEADER/DATETIME	(#PCDATA)
	The date and time of the ticket edit request. The date appears in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).

XPath	element specifications / notes
/TICKET_EDIT_OUTPUT/HEADER/UPDATE	
	((ASSIGNEE?, STATE?, COMMENT?, REOPEN_IGNORED_DAYS?)+)
	The ticket update parameters specified with the ticket_edit.php request are described below.
/TICKET_EDIT_OUTPUT/HEADER/UPDATE/ASSIGNEE (#PCDATA)	
	The user login ID of the current ticket assignee. The ticket assignee was updated by the ticket edit request.
/TICKET_EDIT_OUTPUT/HEADER/UPDATE/STATE (#PCDATA)	
	The current ticket state. The ticket state was updated by the ticket edit request. A possible value is OPEN (for state/status Open and Open/Reopened), RESOLVED (for state Resolved), or IGNORED (for state/status Closed/Ignored).
/TICKET_EDIT_OUTPUT/HEADER/UPDATE/COMMENT (#PCDATA)	
	A ticket comment. This comment was added by the ticket edit request.
/TICKET_EDIT_OUTPUT/HEADER/UPDATE/REOPEN_IGNORED_DAYS (#PCDATA)	
	The number of days when the Closed/Ignored ticket will be reopened. The number was set by the ticket edit request.
/TICKET_EDIT_OUTPUT/HEADER/WHERE	
	((MODIFIED_SINCE_DATETIME?,UNMODIFIED_SINCE_DATETIME?, TICKET_NUMBERS?, SINCE_TICKET_NUMBER?, UNTIL_TICKET_NUMBER?, STATES?, IPS?, ASSET_GROUPS?, DNS_CONTAINS?, NETBIOS_CONTAINS?, VULN_SEVERITIES?, POTENTIAL_VULN_SEVERITIES?, OVERDUE?, INVALID?, TICKET_ASSIGNEE?, QIDS?, VULN_TITLE_CONTAINS?, VULN_DETAILS_CONTAINS?, VENDOR_REF_CONTAINS?) +)
	The ticket selection parameters specified with the ticket_edit.php request are described below.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/MODIFIED_SINCE_DATETIME (#PCDATA)	
	The start date/time of a time window when tickets were modified. The end of the time window is the date/time when the API function was run. Only tickets modified within this time window were selected. The date/time appears in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
/TICKET_EDIT_OUTPUT/HEADER/WHERE/UNMODIFIED_SINCE_DATETIME (#PCDATA)	
	The start date/time of a time window when tickets were not modified. The end of the time window is the date/time when the API function was run. Only tickets that were not modified within this time window were selected. The date/time appears in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
/TICKET_EDIT_OUTPUT/HEADER/WHERE/TICKET_NUMBERS (#PCDATA)	
	One or more ticket numbers and/or ranges were selected. Ticket range start and end is separated by a dash (-).
/TICKET_EDIT_OUTPUT/HEADER/WHERE/SINCE_TICKET_NUMBER (#PCDATA)	
	The lowest ticket number selected. Selected tickets have numbers greater than or equal to the ticket number specified.

XPath	element specifications / notes
/TICKET_EDIT_OUTPUT/HEADER/WHERE/UNTIL_TICKET_NUMBER (#PCDATA)	
	The highest ticket number selected. Selected tickets have numbers less than or equal to the ticket number specified.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/STATES (#PCDATA)	
	The selected ticket states. Possible values are OPEN (for state/status Open or Open/Reopened), RESOLVED (for state Resolved), CLOSED (for state/status Closed/Fixed) and IGNORED (for state/status Closed/Ignored).
/TICKET_EDIT_OUTPUT/HEADER/WHERE/IPS (#PCDATA)	
	The selected IP addresses and/or ranges. Tickets on these IP addresses/ranges were selected.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/ASSET_GROUPS (#PCDATA)	
	The title of one or more selected asset groups. Tickets on IPs in these asset groups were selected.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/DNS_CONTAINS (#PCDATA)	
	A text string contained within the DNS host name. Tickets with a DNS host name containing this text string were selected.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/NETBIOS_CONTAINS (#PCDATA)	
	A text string contained within the NetBIOS host name. Tickets with a NetBIOS host name containing this text string were selected.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/VULN_SEVERITIES (#PCDATA)	
	One or more vulnerability severity levels. Tickets with vulnerabilities having these severity levels were selected.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/POTENTIAL_VULN_SEVERITIES (#PCDATA)	
	One or more potential vulnerability severity levels. Tickets with potential vulnerabilities having these severity levels were selected.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/OVERDUE (#PCDATA)	
	The value 1 indicates that only overdue tickets were selected. The value 0 indicates that only non-overdue tickets were selected.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/INVALID (#PCDATA)	
	The value 1 indicates that only invalid tickets were selected. The value 0 indicates that only valid tickets that were selected.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/TICKET_ASSIGNEE (#PCDATA)	
	The user login of an active account who is the ticket assignee. Tickets with this assignee were selected.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/QIDS (#PCDATA)	
	One or more Qualys IDs (QIDs). Tickets with these QIDs were selected.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/VULN_TITLE_CONTAINS (#PCDATA)	
	A text string contained within the vulnerability title. Tickets with vulnerabilities containing this text string were selected.

XPath	element specifications / notes
/TICKET_EDIT_OUTPUT/HEADER/WHERE/VULN_DETAILS_CONTAINS (#PCDATA)	
	A text string contained within vulnerability details. Tickets with vulnerability details containing this text string were selected.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/VENDOR_REF_CONTAINS (#PCDATA)	
	A text string contained within a vendor reference for the vulnerability. Tickets with a vendor reference containing this text string were selected.

Ticket Edit Output — Changed and Skipped Tickets

XPath	element specifications / notes
/TICKET_EDIT_OUTPUT/CHANGES (TICKET_NUMBER_LIST)	
attribute: **count**	**count** is *implied* and, if present, is the total number of tickets that were edited.
/TICKET_EDIT_OUTPUT/CHANGES/TICKET_NUMBER_LIST (TICKET_NUMBER+)	
/TICKET_EDIT_OUTPUT/CHANGES/TICKET_NUMBER_LIST/TICKET_NUMBER (#PCDATA)	
	The number of a ticket that was changed.
/TICKET_EDIT_OUTPUT/SKIPPED (TICKET_LIST)	
attribute: **count**	**count** is *implied* and, if present, is the total number of tickets that were not changed for some reason.
/TICKET_EDIT_OUTPUT/SKIPPED/TICKET_LIST (TICKET+)	
/TICKET_EDIT_OUTPUT/SKIPPED/TICKET_LIST/TICKET (NUMBER, REASON)	
/TICKET_EDIT_OUTPUT/SKIPPED/TICKET_LIST/TICKET /NUMBER (#PCDATA)	
	The number of a ticket that was not changed for some reason.
/TICKET_EDIT_OUTPUT/SKIPPED/TICKET_LIST/TICKET /REASON (#PCDATA)	
	The reason why the ticket identified in the NUMBER element was not changed. Possible reasons are: “Nothing to change” “Ticket not found (# ticket number)” “Ticket cannot be moved from Closed into Resolved state” “The IP in this ticket is not in the user’s account” “Mid-air collision detected” Note: The "Mid-air collision detected" reason is returned when two Qualys entities (end users, API requests, and/or the service itself) attempts to change a ticket at the same time. In this case, the first request is processed and any additional requests return an error.

Ticket Delete Output

The ticket delete output (ticket_delete_output.dtd) is an XML report returned from the **`ticket_delete.php`** function. This report includes a status message and identifies tickets that were deleted.

DTD for Ticket Delete Output

A recent DTD for the ticket delete output (ticket_delete_output.dtd) is shown below.

```
<!-- QUALYS TICKET DELETE OUTPUT DTD -->

<!ELEMENT TICKET_DELETE_OUTPUT (ERROR | (HEADER, RETURN?)?)>

<!-- Ticket Report error -->
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!-- Information about the Ticket Report -->
<!ELEMENT HEADER (USER_LOGIN, COMPANY, DATETIME, WHERE)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT COMPANY (#PCDATA)>
<!ELEMENT DATETIME (#PCDATA)>

<!-- Search criteria -->
<!ELEMENT WHERE ((MODIFIED_SINCE_DATETIME?, UNMODIFIED_SINCE_DATETIME?,
                  TICKET_NUMBERS?, SINCE_TICKET_NUMBER?,
                  UNTIL_TICKET_NUMBER?, STATES?, IPS?, ASSET_GROUPS?,
                  DNS_CONTAINS?, NETBIOS_CONTAINS?, VULN_SEVERITIES?,
                  POTENTIAL_VULN_SEVERITIES?, OVERDUE?, INVALID?,
                  TICKET_ASSIGNEE?, QIDS?, VULN_TITLE_CONTAINS?,
                  VULN_DETAILS_CONTAINS?,VENDOR_REF_CONTAINS?)+) >
<!ELEMENT MODIFIED_SINCE_DATETIME (#PCDATA)>
<!ELEMENT UNMODIFIED_SINCE_DATETIME (#PCDATA)>
<!ELEMENT TICKET_NUMBERS (#PCDATA)>
<!ELEMENT SINCE_TICKET_NUMBER (#PCDATA)>
<!ELEMENT UNTIL_TICKET_NUMBER (#PCDATA)>
<!ELEMENT STATES (#PCDATA)>
<!ELEMENT IPS (#PCDATA)>
<!ELEMENT ASSET_GROUPS (#PCDATA)>
<!ELEMENT DNS_CONTAINS (#PCDATA)>
<!ELEMENT NETBIOS_CONTAINS (#PCDATA)>
<!ELEMENT VULN_SEVERITIES (#PCDATA)>
<!ELEMENT POTENTIAL_VULN_SEVERITIES (#PCDATA)>
<!ELEMENT OVERDUE (#PCDATA)>
<!ELEMENT INVALID (#PCDATA)>
<!ELEMENT TICKET_ASSIGNEE (#PCDATA)>
<!ELEMENT QIDS (#PCDATA)>
```

```
<!ELEMENT VULN_TITLE_CONTAINS (#PCDATA)>
<!ELEMENT VULN_DETAILS_CONTAINS (#PCDATA)>
<!ELEMENT VENDOR_REF_CONTAINS (#PCDATA)>

<!ELEMENT RETURN (MESSAGE?, CHANGES?)>
<!ATTLIST RETURN
          status (FAILED|SUCCESS|WARNING) #REQUIRED
          number CDATA #IMPLIED>

<!ELEMENT MESSAGE (#PCDATA)>
<!ELEMENT CHANGES (TICKET_NUMBER_LIST)>
<!ATTLIST CHANGES
          count CDATA #REQUIRED>

<!ELEMENT TICKET_NUMBER_LIST (TICKET_NUMBER+)>
<!ELEMENT TICKET_NUMBER (#PCDATA)>
```

XPaths for Ticket Delete Output

This section describes the XPaths for the ticket delete output (ticket_delete_output.dtd).

XPath	element specifications / notes
/TICKET_DELETE_OUTPUT	(ERROR | (HEADER, RETURN?)?)
/TICKET_DELETE_OUTPUT/ERROR (#PCDATA)	
attribute: **number**	**number** is *implied* and, if present, is an error code.
/TICKET_DELETE_OUTPUT/HEADER (USER_LOGIN, COMPANY, DATETIME, WHERE)	
/TICKET_DELETE_OUTPUT/HEADER/USER_LOGIN (#PCDATA)	
	The Qualys user login name for the user who requested the delete function.
/TICKET_DELETE_OUTPUT/HEADER/COMPANY (#PCDATA)	
	The company associated with the Qualys user.
/TICKET_DELETE_OUTPUT/HEADER/DATETIME (#PCDATA)	
	The date and time when the function was run. The date appears in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT) like this: "2005-01-10T02:33:11Z".
/TICKET_DELETE_OUTPUT/HEADER/WHERE	
	((MODIFIED_SINCE_DATETIME?, UNMODIFIED_SINCE_DATETIME?, TICKET_NUMBERS?, SINCE_TICKET_NUMBER?, UNTIL_TICKET_NUMBER?, STATES?, IPS?, ASSET_GROUPS?, DNS_CONTAINS?, NETBIOS_CONTAINS?, VULN_SEVERITIES?, POTENTIAL_VULN_SEVERITIES?, OVERDUE?, INVALID?, TICKET_ASSIGNEE?, QIDS?, VULN_TITLE_CONTAINS?, VULN_DETAILS_CONTAINS?, VENDOR_REF_CONTAINS?) +)
	The ticket selection parameters specified with the ticket_delete.php request are described below.

XPath	element specifications / notes
/TICKET_DELETE_OUTPUT/HEADER/WHERE/MODIFIED_SINCE_DATETIME (#PCDATA)	
	The start date/time of a time window when tickets were modified. The end of the time window is the date/time when the API function was run. Only tickets modified within this time window were selected. The start date/time appears in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
/TICKET_DELETE_OUTPUT/HEADER/WHERE/UNMODIFIED_SINCE_DATETIME (#PCDATA)	
	The start date/time of the time window when tickets were not modified. The end of the time window is the date/time when the API function was run. Only tickets that were not modified within this time window were retrieved. The start date/time appears in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
/TICKET_DELETE_OUTPUT/HEADER/WHERE/TICKET_NUMBERS (#PCDATA)	
	One or more ticket numbers and/or ranges. Ticket range start and end is separated by a dash (-).
/TICKET_DELETE_OUTPUT/HEADER/WHERE/SINCE_TICKET_NUMBER (#PCDATA)	
	The lowest ticket number selected. Selected tickets have numbers greater than or equal to the ticket number specified.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/UNTIL_TICKET_NUMBER (#PCDATA)	
	The highest ticket number selected. Selected tickets have numbers less than or equal to the ticket number specified.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/STATES (#PCDATA)	
	The selected ticket states. Possible values are OPEN (for state/status Open or Open/Reopened), RESOLVED (for state Resolved), CLOSED (for state/status Closed/Fixed) and IGNORED (for state/status Closed/Ignored).
/TICKET_DELETE_OUTPUT/HEADER/WHERE/IPS (#PCDATA)	
	The selected IP addresses and/or ranges. Tickets on these IP addresses and/or ranges were selected.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/ASSET_GROUPS (#PCDATA)	
	The title of one or more selected asset groups. Tickets on IP addresses in these asset groups were selected.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/DNS_CONTAINS (#PCDATA)	
	A text string contained within the DNS host name. Tickets with a DNS host name containing this string were selected.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/NETBIOS_CONTAINS (#PCDATA)	
	A text string contained within the NetBIOS host name. Tickets with a NetBIOS host name containing this string were selected.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/VULN_SEVERITIES (#PCDATA)	
	One or more vulnerability severity levels. Tickets with vulnerabilities having these severity levels were selected.

XPath	element specifications / notes
/TICKET_DELETE_OUTPUT/HEADER/WHERE/POTENTIAL_VULN_SEVERITIES (#PCDATA)	
	One or more potential vulnerability severity levels. Tickets with potential vulnerabilities having these severity levels were selected.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/OVERDUE (#PCDATA)	
	The value 1 indicates that only overdue tickets were selected. The value 0 indicates that only non-overdue tickets were selected.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/INVALID (#PCDATA)	
	The value 1 indicates that only invalid tickets were selected. The value 0 indicates that only valid tickets were selected.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/TICKET_ASSIGNEE (#PCDATA)	
	The user login of an active account who is the ticket assignee. Tickets with this assignee were selected.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/QIDS (#PCDATA)	
	One or more Qualys IDs (QIDs). Tickets with these QIDs were selected.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/VULN_TITLE_CONTAINS (#PCDATA)	
	A text string contained within the vulnerability title. Tickets with vulnerabilities containing this text string were selected.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/VULN_DETAILS_CONTAINS (#PCDATA)	
	A text string contained within vulnerability details. Tickets with vulnerability details containing this text string were selected.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/VENDOR_REF_CONTAINS (#PCDATA)	
	A text string contained within a vendor reference for the vulnerability. Tickets with a vendor reference containing this text string were selected.
/TICKET_DELETE_OUTPUT/RETURN (MESSAGE?, CHANGES?)	
attribute: **status**	**status** is *required* and is a status code, either SUCCESS, FAILED, or WARNING.
attribute: **number**	**number** is *implied* and, if present, is an error code.
/TICKET_DELETE_OUTPUT/RETURN/MESSAGE (#PCDATA)	
	A descriptive message that corresponds to the status code.
/TICKET_DELETE_OUTPUT/RETURN/CHANGES (TICKET_NUMBER_LIST)	
attribute: **count**	**count** is *implied* and, if present, is the total number of tickets that were deleted.
/TICKET_DELETE_OUTPUT/RETURN/CHANGES/TICKET_NUMBER_LIST (TICKET_NUMBER+)	
/TICKET_DELETE_OUTPUT/RETURN/CHANGES/TICKET_NUMBER_LIST/TICKET_NUMBER (#PCDATA)	
	A single ticket number that was deleted.

Deleted Ticket List

The deleted ticket list output (ticket_list_deleted_output.dtd) is an XML report returned from the **ticket_list_deleted.php** function. This report includes a status message and identifies tickets that were changed.

DTD for Deleted Ticket List Output

A recent DTD for the deleted ticket list output (ticket_list_deleted_output.dtd) is shown below.

```
<!-- QUALYS TICKET LIST DELETED OUTPUT DTD -->

<!ELEMENT TICKET_LIST_DELETED_OUTPUT
((HEADER,(TICKET_LIST|ERROR|TRUNCATION)*) | ERROR)>

<!-- Ticket Report error -->
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!-- Truncation warning -->
<!ELEMENT TRUNCATION (#PCDATA)>
<!ATTLIST TRUNCATION last CDATA #IMPLIED>

<!-- Information about the Ticket Report -->
<!ELEMENT HEADER (USER_LOGIN, COMPANY, DATETIME, WHERE)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT COMPANY (#PCDATA)>
<!ELEMENT DATETIME (#PCDATA)>

<!-- Search criteria -->
<!ELEMENT WHERE ((DELETED_SINCE_DATETIME?,DELETED_BEFORE_DATETIME?,
                  SINCE_TICKET_NUMBER?, UNTIL_TICKET_NUMBER?,
                  TICKET_NUMBERS?)+)>
<!ELEMENT DELETED_SINCE_DATETIME (#PCDATA)>
<!ELEMENT DELETED_BEFORE_DATETIME (#PCDATA)>
<!ELEMENT SINCE_TICKET_NUMBER (#PCDATA)>
<!ELEMENT UNTIL_TICKET_NUMBER (#PCDATA)>
<!ELEMENT TICKET_NUMBERS (#PCDATA)>

<!-- Ticket information -->
<!ELEMENT TICKET_LIST (TICKET+)>
<!ELEMENT TICKET (NUMBER, DELETION_DATETIME)>
<!ELEMENT NUMBER (#PCDATA)>
<!ELEMENT DELETION_DATETIME (#PCDATA)>
```

XPaths for Deleted Ticket List Output

This section describes the XPaths for the deleted tickets list output (ticket_list_deleted_output.dtd).

Deleted Ticket List — Header Information

XPath	element specifications / notes
/TICKET_LIST_DELETED_OUTPUT	
	((HEADER,(TICKET_LIST|ERROR|TRUNCATION)*) | ERROR)
/TICKET_LIST_DELETED_OUTPUT/ERROR (#PCDATA)	
attribute: **number**	**number** is *implied* and if present, is an error code.
/TICKET_LIST_DELETED_OUTPUT/TRUNCATION (#PCDATA)	
attribute: **last**	**last** is *implied* and if present, is the last ticket number included in the deleted ticket list. This list is truncated after 1000 records.
/TICKET_LIST_DELETED_OUTPUT/HEADER	
	(USER_LOGIN, COMPANY, DATETIME, WHERE)
/TICKET_LIST_DELETED_OUTPUT/HEADER/USER_LOGIN	
	The Qualys user login for the user that requested the deleted ticket list.
/TICKET_LIST_DELETED_OUTPUT/HEADER/COMPANY	
	The company associated with the Qualys user.
/TICKET_LIST_DELETED_OUTPUT/HEADER/DATETIME	
	The date and time when the ticket list report was requested, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/TICKET_LIST_DELETED_OUTPUT/HEADER/WHERE	
	((DELETED_SINCE_DATETIME?, DELETED_BEFORE_DATETIME?, SINCE_TICKET_NUMBER?, UNTIL_TICKET_NUMBER?, TICKET_NUMBERS?) +)
	Ticket selection parameters specified as part of the ticket_list_deleted.php request.
/TICKET_LIST_DELETED_OUTPUT/HEADER/WHERE/DELETED_SINCE_DATETIME (#PCDATA)	
	Tickets deleted since this date/time, in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
/TICKET_LIST_DELETED_OUTPUT/HEADER/WHERE/DELETED_BEFORE_DATETIME (#PCDATA)	
	Tickets deleted since this date/time, in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
/TICKET_LIST_DELETED_OUTPUT/HEADER/WHERE/SINCE_TICKET_NUMBER (#PCDATA)	
	Tickets since this ticket number. Selected tickets will have numbers greater than or equal to the ticket number specified.
/TICKET_LIST_DELETED_OUTPUT/HEADER/WHERE/UNTIL_TICKET_NUMBER (#PCDATA)	
	Tickets until this ticket number. Selected tickets will have numbers less than or equal to the ticket number specified.

XPath	element specifications / notes
/TICKET_LIST_DELETED_OUTPUT/HEADER/WHERE/TICKET_NUMBERS (#PCDATA)	
	Tickets with certain ticket numbers. One or more ticket numbers and/or ranges. Ticket range start and end is separated by a dash (-).

Deleted Ticket List — General Ticket Information

XPath	element specifications / notes
/TICKET_LIST_DELETED_OUTPUT/TICKET_LIST (TICKET+)	
/TICKET_LIST_DELETED_OUTPUT/TICKET_LIST/TICKET (NUMBER, DELETION_DATETIME)	
/TICKET_LIST_DELETED_OUTPUT/TICKET_LIST/TICKET/NUMBER (#PCDATA)	
	The total number of deleted tickets.
/TICKET_LIST_DELETED_OUTPUT/TICKET_LIST/TICKET/DELETION_DATETIME (#PCDATA)	
	The date when the ticket was deleted, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).

Get Ticket Information Report

The get ticket information report (remediation_tickets.dtd) is an XML report returned from the **`get_tickets.php`** function. This report includes information about remediation tickets available in the user's Qualys account.

DTD for Get Ticket Information Report

A recent DTD for the get ticket information report (remediation_tickets.dtd) is shown below.

```
<!-- QUALYS REMEDIATION TICKET INFO DTD -->
<!ELEMENT REMEDIATION_TICKETS ((HEADER,ACCOUNT,(TICKET|ERROR)*) | ERROR)
>

<!-- Ticket Report error -->
<!ELEMENT ERROR (#PCDATA) >
<!ATTLIST ERROR number CDATA #IMPLIED >

<!-- Information about the Ticket Report -->
<!ELEMENT HEADER (KEY+) >
<!-- Header Keys, e.g.
        USERNAME: corp_xxn
        COMPANY: <![CDATA[corp name]]>
        DATE: yyyy-dd-mm-ddThh-mm-ssZ
-->

<!ELEMENT KEY (#PCDATA) >
<!ATTLIST KEY
          value CDATA #IMPLIED >

<!-- Account information -->
<!ELEMENT ACCOUNT EMPTY >
<!ATTLIST ACCOUNT
          account-id CDATA #REQUIRED>

<!ELEMENT TICKET (ASSIGNEE+,HOST,STATS?,HISTORY+,VULNINFO?,DETAILS?) >
<!ATTLIST TICKET
          number NMTOKEN #REQUIRED
          created CDATA #IMPLIED
          due CDATA #IMPLIED
          state CDATA #REQUIRED
          status CDATA #IMPLIED
          ticket-id CDATA #REQUIRED
>
```

```
<!-- Ticket Assignee - content is QualysGuard user login ID -->
<!ELEMENT ASSIGNEE (#PCDATA) >
<!ATTLIST ASSIGNEE
          name CDATA #REQUIRED
          email CDATA #REQUIRED
>

<!-- Target Asset -->
<!ELEMENT HOST (DNSNAME?,NBHNAME?,PORT?,SERVICE?,PROTOCOL?,FQDN?,SSL?) >
<!ATTLIST HOST
        ip CDATA #REQUIRED>
<!-- DNS Hostname -->
<!ELEMENT DNSNAME (#PCDATA) >
<!-- NetBios Hostname -->
<!ELEMENT NBHNAME (#PCDATA) >
<!-- TCP Port of the vuln -->
<!ELEMENT PORT (#PCDATA) >
<!-- service name on the host-->
<!ELEMENT SERVICE (#PCDATA) >
<!-- Protocol -->
<!ELEMENT PROTOCOL (#PCDATA) >
<!-- FQDN -->
<!ELEMENT FQDN (#PCDATA) >
<!-- was this found using SSL -->
<!ELEMENT SSL (#PCDATA) >

<!-- Ticket Statistics -->
<!ELEMENT STATS EMPTY >
<!ATTLIST STATS
        first-found CDATA #REQUIRED
        last-found CDATA #REQUIRED
        last-scan CDATA #REQUIRED
        times-found CDATA #REQUIRED
        times-not-found CDATA #REQUIRED
        last-open CDATA #REQUIRED
        last-resolved CDATA #IMPLIED
        last-closed CDATA #IMPLIED
        last-ignored CDATA #IMPLIED
>

<!-- Ticket History -->
<!ELEMENT HISTORY
(STATE?,ADDED_ASSIGNEES?,REMOVED_ASSIGNEES?,SCAN?,RULE?,COMMENT?) >
<!ATTLIST HISTORY
        added NMTOKEN #REQUIRED
        by CDATA #REQUIRED>

<!-- Ticket state/status -->
<!ELEMENT STATE EMPTY >
```

```
<!ATTLIST STATE
          old-state CDATA #IMPLIED
          new-state CDATA #IMPLIED>

<!-- added assignees -->
<!ELEMENT ADDED_ASSIGNEES (ASSIGNEE+) >

<!-- added assignees -->
<!ELEMENT REMOVED_ASSIGNEES (ASSIGNEE+) >

<!-- Scan Report that triggered ticket policy -->
<!ELEMENT SCAN EMPTY >
<!ATTLIST SCAN
          ref CDATA #REQUIRED
          date CDATA #REQUIRED
>

<!-- Ticket Creation Rule (Policy) -->
<!ELEMENT RULE (#PCDATA) >

<!-- Ticket Comment -->
<!ELEMENT COMMENT (#PCDATA) >

<!-- Ticket Vulnerability Information -->
<!ELEMENT VULNINFO (TITLE,CVE*,VENDOR*)>
<!-- severity is Qualys severity level 1 to 5 (possibly customized)  -->

<!--
     standard-severity is the original Qualys severity level 1 to 5
     if it has been customized by the user
-->
<!ATTLIST VULNINFO
          type (VULN|POSS) #REQUIRED
          qid CDATA #REQUIRED
          severity CDATA #REQUIRED
          standard-severity CDATA #IMPLIED
>

<!-- CVE ID and optional URI to CVE website -->
<!ELEMENT CVE (#PCDATA) >
<!ATTLIST CVE
        id CDATA #REQUIRED
>
<!--
    Vendor Reference and optional URI to vendor website,
    e.g. name and location of vendor patch from Microsoft, RedHat, SUSE,
Sun
-->
<!ELEMENT VENDOR (#PCDATA) >
```

```
<!ATTLIST VENDOR
        ref CDATA #REQUIRED>
<!ELEMENT TITLE (#PCDATA) >

<!-- Ticket Vulnerability Details -->
<!ELEMENT DETAILS
(DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,CORRELATION?,RESULT?)>

<!ELEMENT DIAGNOSIS (#PCDATA) >
<!ELEMENT CONSEQUENCE (#PCDATA) >
<!ELEMENT SOLUTION (#PCDATA) >
<!ELEMENT CORRELATION (EXPLOITABILITY?,MALWARE?)>
<!ELEMENT EXPLOITABILITY (EXPLT_SRC)+>
<!ELEMENT EXPLT_SRC (SRC_NAME, EXPLT_LIST)>
<!ELEMENT SRC_NAME (#PCDATA)>
<!ELEMENT EXPLT_LIST (EXPLT)+>
<!ELEMENT EXPLT (REF, DESC, LINK?)>
<!ELEMENT REF (#PCDATA)>
<!ELEMENT DESC (#PCDATA)>
<!ELEMENT LINK (#PCDATA)>

<!ELEMENT MALWARE (MW_SRC)+>
<!ELEMENT MW_SRC (SRC_NAME, MW_LIST)>
<!ELEMENT MW_LIST (MW_INFO)+>
<!ELEMENT MW_INFO (MW_ID, MW_TYPE?, MW_PLATFORM?, MW_ALIAS?, MW_RATING?,
                   MW_LINK?)>
<!ELEMENT MW_ID (#PCDATA)>
<!ELEMENT MW_TYPE (#PCDATA)>
<!ELEMENT MW_PLATFORM (#PCDATA)>
<!ELEMENT MW_ALIAS (#PCDATA)>
<!ELEMENT MW_RATING (#PCDATA)>
<!ELEMENT MW_LINK (#PCDATA)>
<!ELEMENT RESULT (#PCDATA) >
<!--
    If the "format" attribute is set to "table", then column
    values are separated by tab '\t', and rows are terminated
    by new line '\n'.
-->
<!ATTLIST RESULT
          format CDATA #IMPLIED
>
```

XPaths for Ticket Information Report

This section describes the XPaths for the ticket information report (remediation_tickets.dtd).

Tickets — Header Information

XPath	element specifications / notes
/REMEDIATION_TICKETS	((HEADER,ACCOUNT,TICKET*) | ERROR)
/REMEDIATION_TICKETS/HEADER	(KEY)+
/REMEDIATION_TICKETS/HEADER/KEY	
attribute: **value**	**value** is *implied* and, if present, will be one of the following: USERNAME..... The Qualys user login name for the user that requested the ticket report. COMPANY..... The company associated with the Qualys user. DATE..... The date when the ticket report was requested in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/REMEDIATION_TICKETS/ACCOUNT	
attribute: **account-id**	**account-id** is *required* and will be the MD5 hash of the Qualys subscription ID associated with the Qualys user account specified in the header key USERNAME.
/REMEDIATION_TICKETS/ERROR	
attribute: **number**	**number** is *implied* and, if present, is an error code.

Tickets — General Ticket Information

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET	(ASSIGNEE+,HOST,STATS?,HISTORY+,VULNINFO?,DETAILS?)
attribute: **number**	**value** is *required* and is the remediation ticket number that appears in the Qualys user interface.
attribute: **created**	**created** is *implied*, and if present, will be the date when the ticket was first created in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
attribute: **due**	**due** is *implied*, and if present, will be the due date for ticket resolution in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
attribute: **state**	**state** is *required* and will be the current ticket state: OPEN, RESOLVED, or CLOSED.
attribute: **status**	**status** is *implied*, and if present, will be the current ticket status: REOPENED, FIXED, IGNORED.
attribute: **ticket-id**	**ticket-id** is *required* and will be the unique ID of the remediation ticket, used to identify the ticket within the Qualys application.

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET/ASSIGNEE	
	The user login name of the assignee's Qualys user account.
attribute: **name**	**name** is *required* and is the full name (first and last) of the assignee, as defined in the assignee's Qualys user account.
attribute: **email**	**email** is *required* and is the email address of the assignee, as defined in the assignee's Qualys user account.
/REMEDIATION_TICKETS/TICKET/COMMENT	
	Comments added to the ticket by Qualys users.

Tickets — Host Information

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET/HOST	
	(DNSNAME?,NBHNAME?,PORT?,SERVICE?,PROTOCOL?,FQDN?,SSL?)
attribute: **ip**	**ip** is *required* and is the IP address that the ticket applies to, the IP address on which the vulnerability was detected.
/REMEDIATION_TICKETS/TICKET/HOST/DNSNAME	
	The registered DNS host name.
/REMEDIATION_TICKETS/TICKET/HOST/NBHNAME	
	The Microsoft Windows NetBIOS host name.
/REMEDIATION_TICKETS/TICKET/HOST/PORT	
	The TCP port on which the vulnerability was detected.
/REMEDIATION_TICKETS/TICKET/HOST/SERVICE	
	The service name of the host, found during information gathering.
/REMEDIATION_TICKETS/TICKET/HOST/PROTOCOL	
	The protocol running on the host, when known.
/REMEDIATION_TICKETS/TICKET/HOST/FQDN	
	The fully qualified domain name of the host, when known.
/REMEDIATION_TICKETS/TICKET/HOST/SSL	
	A flag indicating whether SSL was present on this host when known. If SSL was present, the SSL element appears with the value TRUE.

Tickets — Statistics and History

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET/STATS	
attribute: **first-found**	**first-found** is *required* and will be the date and time when the vulnerability was first detected on the host, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT)
attribute: **last-found**	**last-found** is *required* and will be the date and time when the vulnerability was last detected on the host (from the most recent scan), in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT)
attribute: **last-scan**	**last-scan** is *required* and will be the date and time of the most recent scan of the host, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT)
attribute: **times-found**	**times-found** is *required* and will be the total number of times the vulnerability was detected on the host
attribute: **times-not-found**	**times-not-found** is *required* and will be the total number of times the host was scanned and the vulnerability not detected
attribute: **last-open**	**last-open** is *required* and will be the date of the most recent scan which caused the ticket state to be changed to Open, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT)
attribute: **last-resolved**	**last-resolved** is *implied*, and if present, will be the date of the most recent scan which caused the ticket state to be changed to Resolved, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT)
attribute: **last-closed**	**last-closed** is *implied*, and if present, will be the date of the most recent scan which caused the ticket state to be changed to Closed, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT)
attribute: **last-ignored**	**last-ignored** is *implied*, and if present, will be the most recent date and time when the ticket was marked as Ignored, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT)
/REMEDIATION_TICKETS/TICKET/HISTORY	
	(STATE?,ADDED_ASSIGNEES?,REMOVED_ASSIGNEES?,SCAN?,RULE?,COMMENT?)
attribute: **added**	**added** is *required* and is the token name for the ticket history event
attribute: **by**	**by** is *required* and is the Qualys user login name, identifying the user whose action prompted the ticket history event (such as user scan resulting in ticket state/status change, user ticket edit)
/REMEDIATION_TICKETS/TICKET/HISTORY/STATE	
attribute: **old-state**	**old-state** is *implied*, and if present, will be the old (previous) state of the ticket
attribute: **new-state**	**new-state** *implied*, and if present, will be the new state of the ticket
/REMEDIATION_TICKETS/TICKET/HISTORY/ADDED_ASSIGNEES	
	Qualys user login name of an assignee that was added.
/REMEDIATION_TICKETS/TICKET/HISTORY/REMOVED_ASSIGNEES	
	Qualys user login name of an assignee that was removed.

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET/HISTORY/SCAN	
attribute: **ref**	**ref** is *required* and is the scan report reference for the scan that triggered the ticket update event. Note: For a new ticket created by a user, a scan report reference is not returned.
attribute: **date**	**date** is *required* and is the date and time of the scan that triggered the ticket update event, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT)
/REMEDIATION_TICKETS/TICKET/HISTORY/RULE	
	The name of the policy rule that triggered the automatic ticket creation.

Tickets — Vulnerability Information

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET/VULNINFO	
	(TITLE,CVE*,VENDOR*)
attribute: **type**	**type** is *required* and is a vulnerability type flag, VULN for vulnerability and POSS for potential vulnerability
attribute: **qid**	**qid** is *required* and is the Qualys ID number assigned to the vulnerability
attribute: **severity**	**severity** is *required* and is the Qualys assigned severity level (from 1 to 5)
attribute: **standard-severity**	**standard-severity** is *implied*, and if present, will be a user-defined severity level (from 1 to 5)
/REMEDIATION_TICKETS/TICKET/VULNINFO/TITLE	
	The title of the vulnerability as defined for the vulnerability in the Qualys Vulnerability KnowledgeBase.
/REMEDIATION_TICKETS/TICKET/VULNINFO/CVE	
	CVE (Common Vulnerabilities and Exposures) is a list of common names for publicly known vulnerabilities and exposures. Through open and collaborative discussions, the CVE Editorial Board determines which vulnerabilities or exposures are included in CVE. If the CVE name starts with CAN (candidate) then it is under consideration for entry into CVE.
attribute: **id**	**id** is *required* and is the CVE name(s) associated with the Qualys vulnerability check associated with the ticket
/REMEDIATION_TICKETS/TICKET/VULNINFO/VENDOR	
	URI to the vendor Web site, when available
attribute: **ref**	**ref** is *required* and is a vendor reference name, like Microsoft, Red Hat, SUSE, Sun
/REMEDIATION_TICKETS/TICKET/DETAILS	
	(DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,CORRELATION?,RESULT?)
/REMEDIATION_TICKETS/TICKET/DETAILS/DIAGNOSIS	
	A description of the threat posted by the vulnerability, from the Qualys KnowledgeBase. This element may be present only when **get_tickets.php** is specified with the **vuln_details=1** parameter.

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET/DETAILS/CONSEQUENCE	
	A description of the possible impact if the vulnerability is exploited, from the Qualys KnowledgeBase. This element may be present only when **`get_tickets.php`** is specified with the **`vuln_details=1`** parameter.
/REMEDIATION_TICKETS/TICKET/DETAILS/SOLUTION	
	A verified solution to fix the vulnerability, from the Qualys KnowledgeBase. When virtual patch information is correlated with a vulnerability, the virtual patch information from Trend Micro appears under the heading "Virtual Patches:". This includes a list of virtual patches and a link to more information. This element may be present only when **`get_tickets.php`** is specified with the **`vuln_details=1`** parameter.
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION	(EXPLOITABILITY?, MALWARE?)
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/EXPLOITABILITY	(EXPLT_SRC)+
	The <EXPLOITABILITY> element and its sub-elements appear only when there is exploitability information for the vulnerability from third party vendors and/or publicly available sources.
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC	(SRC_NAME, EXPLT_LIST)
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/SRC_NAME	(#PCDATA)
	The name of a third party vendor or publicly available source of the vulnerability information.
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST	(EXPLT)+
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT	(REF, DESC, LINK?)
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/REF	(#PCDATA)
	The CVE reference for the exploitability information.
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/DESC	(#PCDATA)
	The description provided by the source of the exploitability information (third party vendor or publicly available source).
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/LINK	(#PCDATA)
	A link to the exploit, when available.
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/MALWARE	(MW_SRC)+
	The <MALWARE> element and its sub-elements appear only when there is malware information for the vulnerability from Trend Micro.
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/MALWARE/MW_SRC	(SRC_NAME, MW_LIST)

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/ MALWARE/MW_SRC/SRC_NAME (#PCDATA)	
	The name of the source of the malware information: Trend Micro.
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/ MALWARE/MW_SRC/MW_LIST (MW_INFO)+	
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/ MALWARE/MW_SRC/MW_LIST/MW_INFO	(MW_ID, MW_TYPE?, MW_PLATFORM?, MW_ALIAS?, MW_RATING?, MW_LINK?)
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/ MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_ID (#PCDATA)	
	The malware name/ID assigned by Trend Micro.
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/ MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_TYPE (#PCDATA)	
	The type of malware, such as Backdoor, Virus, Worm or Trojan.
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/ MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_PLATFORM (#PCDATA)	
	A list of the platforms that may be affected by the malware.
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/ MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_ALIAS (#PCDATA)	
	A list of other names used by different vendors and/or publicly available sources to refer to the same threat.
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/ MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_RATING (#PCDATA)	
	The overall risk rating as determined by Trend Micro: Low, Medium or High.
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/ MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_LINK (#PCDATA)	
	A link to malware details.
/REMEDIATION_TICKETS/TICKET/DETAILS/RESULT	
	Specific scan test results for the vulnerability, from the host assessment data. This element may be present only when **`get_tickets.php`** is specified with the **`vuln_details=1`** parameter.
attribute: **`format`**	**`format`** is *implied* and if present, will be the result format

Get Host Information Report

The get host information report (get_host_info.dtd) is an XML report returned from the **`get_host_info.php`** function. This report identifies a specific host and provides additional host-related information for network security management, such as the host's vulnerability status, latest assessment data and user configurations.

The host information report content varies based on whether parameters are specified for the **`get_host_info.php`** function. When no parameters are specified, the function returns host identification information as well as vulnerability and ticket counts by severity level. Included are current vulnerabilities as well as tickets with Open and Resolved status.

When a **`get_host_info.php`** request includes one or more parameters, additional content is included. See the referenced sections below for further details.

Request type	Report content (see referenced sections)
All requests	"Host — Header Information" "Host — Vulnerability Counts" "Host — Ticket Information"
general_info=1	"Host — General Information"
vuln_details=1	"Host — Vulnerability Information" "Host — Vulnerability References" "CVSS Scoring Information"
ticket_details=1	"Host — Ticket Information"

DTD for Get Host Information Report

A recent DTD for the get host information report (get_host_info.dtd) is shown below.

```
<!-- QUALYS HOST INFO DTD -->
<!ELEMENT HOST (ERROR | (TRACKING_METHOD, SECURITY_RISK, IP,
                         DNS?, NETBIOS?, OPERATING_SYSTEM?,
                         LAST_SCAN_DATE?, COMMENT?,
                         OWNER?, USER_DEFINED_ATTR_LIST?, USER_LIST?,
                         ASSET_GROUP_LIST?, AUTHENTICATION_RECORD_LIST?,
                         BUSINESS_UNIT_LIST?, VULNS?, POTENTIAL_VULNS?,
                         INFO_GATHERED?, TICKETS?))>

<!ELEMENT ERROR (#PCDATA)*>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!-- ================ HOST INFORMATION ================ -->
```

```
<!-- Required elements -->

<!ELEMENT TRACKING_METHOD (#PCDATA)> <!-- IP address | DNS hostname |
NETBIOS hostname -->
<!ELEMENT SECURITY_RISK (#PCDATA)>   <!-- INT 1-5 -->
<!ELEMENT IP (#PCDATA)>

<!-- Optional elements -->

<!ELEMENT DNS (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT OPERATING_SYSTEM (#PCDATA)>
<!ELEMENT LAST_SCAN_DATE (#PCDATA)>
<!ELEMENT COMMENT (#PCDATA)>

<!ELEMENT OWNER (USER)>
<!ELEMENT USER (FIRSTNAME?, LASTNAME?, USER_LOGIN?)>
<!ELEMENT FIRSTNAME (#PCDATA)>
<!ELEMENT LASTNAME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>

<!ELEMENT USER_DEFINED_ATTR_LIST (USER_DEFINED_ATTR+)>
<!ELEMENT USER_DEFINED_ATTR (UDA_INDEX, UDA_TITLE, UDA_VALUE)>
<!ELEMENT UDA_INDEX (#PCDATA)>
<!ELEMENT UDA_TITLE (#PCDATA)>
<!ELEMENT UDA_VALUE (#PCDATA)>

<!ELEMENT USER_LIST (USER+)>

<!ELEMENT ASSET_GROUP_LIST (ASSET_GROUP+)>
<!ELEMENT ASSET_GROUP (ASSET_GROUP_TITLE?,CVSS_ENVIRONMENT?)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>

<!ELEMENT AUTHENTICATION_RECORD_LIST (AUTH_WINDOWS?, AUTH_UNIX?,
                                      AUTH_ORACLE?, AUTH_SNMP?)>
<!ELEMENT AUTH_WINDOWS (#PCDATA)>
<!ELEMENT AUTH_UNIX (#PCDATA)>
<!ELEMENT AUTH_ORACLE (#PCDATA)>
<!ELEMENT AUTH_SNMP (#PCDATA)>

<!ELEMENT BUSINESS_UNIT_LIST (BUSINESS_UNIT+)>
<!ELEMENT BUSINESS_UNIT (#PCDATA)>

<!-- ============ VULN COUNT INFO AND LIST ============== -->

<!ELEMENT VULNS           (SEVERITY_LEVEL_1?, SEVERITY_LEVEL_2?,
                           SEVERITY_LEVEL_3?, SEVERITY_LEVEL_4?,
                           SEVERITY_LEVEL_5?)>
<!ELEMENT POTENTIAL_VULNS (SEVERITY_LEVEL_1?, SEVERITY_LEVEL_2?,
```

```
                            SEVERITY_LEVEL_3?, SEVERITY_LEVEL_4?,
                            SEVERITY_LEVEL_5?)>
<!ELEMENT INFO_GATHERED   (SEVERITY_LEVEL_1?, SEVERITY_LEVEL_2?,
                            SEVERITY_LEVEL_3?, SEVERITY_LEVEL_4?,
                            SEVERITY_LEVEL_5?)>

<!ELEMENT SEVERITY_LEVEL_1 (COUNT, (VULNINFO* | TICKET_NUMBER*))>
<!ELEMENT SEVERITY_LEVEL_2 (COUNT, (VULNINFO* | TICKET_NUMBER*))>
<!ELEMENT SEVERITY_LEVEL_3 (COUNT, (VULNINFO* | TICKET_NUMBER*))>
<!ELEMENT SEVERITY_LEVEL_4 (COUNT, (VULNINFO* | TICKET_NUMBER*))>
<!ELEMENT SEVERITY_LEVEL_5 (COUNT, (VULNINFO* | TICKET_NUMBER*))>

<!ELEMENT COUNT (#PCDATA)>

<!-- ===== VULN INFORMATION ===== -->

<!-- Note that VULN_STATUS does not apply to IGs -->
<!ELEMENT VULNINFO (QID, SEVERITY_LEVEL, TITLE,
                    VULN_STATUS?, CATEGORY?, PORT?, SERVICE?, PROTOCOL?,
                    INSTANCE?, CVSS_SCORE?, FIRST_FOUND?, LAST_FOUND?,
                    TIMES_FOUND?, VENDOR_REFERENCE_LIST?, CVE_ID_LIST?,
                    BUGTRAQ_ID_LIST?, LAST_UPDATE?, DIAGNOSIS?,
                    DIAGNOSIS_COMMENT?, CONSEQUENCE?,
                    CONSEQUENCE_COMMENT?, SOLUTION?, SOLUTION_COMMENT?,
                    COMPLIANCE?, CORRELATION?, RESULT?)>

<!-- Required Elements -->

<!ELEMENT QID (#PCDATA)>
<!ELEMENT SEVERITY_LEVEL (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>

<!-- Optional Elements -->

<!ELEMENT VULN_STATUS (#PCDATA)>
<!ELEMENT CATEGORY (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT SERVICE (#PCDATA)>
<!ELEMENT PROTOCOL (#PCDATA)>
<!ELEMENT INSTANCE (#PCDATA)>
<!ELEMENT CVSS_SCORE (CVSS_BASE?, CVSS_TEMPORAL?, CVSS_ENVIRONMENT?)>
<!ELEMENT CVSS_BASE (#PCDATA)>
<!ATTLIST CVSS_BASE
    source CDATA #IMPLIED
>
<!ELEMENT CVSS_TEMPORAL (#PCDATA)>
<!ELEMENT CVSS_ENVIRONMENT (CVSS_COLLATERAL_DAMAGE_POTENTIAL,
                            CVSS_TARGET_DISTRIBUTION,
                            CVSS_ENV_CR,
```

```
                              CVSS_ENV_IR,
                              CVSS_ENV_AR)>

<!ELEMENT CVSS_COLLATERAL_DAMAGE_POTENTIAL (#PCDATA)>
<!ELEMENT CVSS_TARGET_DISTRIBUTION (#PCDATA)>
<!ELEMENT CVSS_ENV_CR (#PCDATA)>
<!ELEMENT CVSS_ENV_IR (#PCDATA)>
<!ELEMENT CVSS_ENV_AR (#PCDATA)>

<!ELEMENT FIRST_FOUND (#PCDATA)>
<!ELEMENT LAST_FOUND (#PCDATA)>
<!ELEMENT TIMES_FOUND (#PCDATA)>

<!ELEMENT VENDOR_REFERENCE_LIST (VENDOR_REFERENCE+)>
<!ELEMENT VENDOR_REFERENCE (ID,URL)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT URL (#PCDATA)>

<!ELEMENT CVE_ID_LIST (CVE_ID+)>
<!ELEMENT CVE_ID (ID,URL)>

<!ELEMENT BUGTRAQ_ID_LIST (BUGTRAQ_ID+)>
<!ELEMENT BUGTRAQ_ID (ID,URL)>

<!ELEMENT LAST_UPDATE (#PCDATA)>

<!ELEMENT DIAGNOSIS (#PCDATA)>
<!ELEMENT DIAGNOSIS_COMMENT (#PCDATA)>
<!ELEMENT CONSEQUENCE (#PCDATA)>
<!ELEMENT CONSEQUENCE_COMMENT (#PCDATA)>
<!ELEMENT SOLUTION (#PCDATA)>
<!ELEMENT SOLUTION_COMMENT (#PCDATA)>

<!ELEMENT COMPLIANCE (COMPLIANCE_INFO+)>
<!ELEMENT COMPLIANCE_INFO (COMPLIANCE_TYPE, COMPLIANCE_SECTION,
                           COMPLIANCE_DESCRIPTION)>
<!ELEMENT COMPLIANCE_TYPE (#PCDATA)>
<!ELEMENT COMPLIANCE_SECTION (#PCDATA)>
<!ELEMENT COMPLIANCE_DESCRIPTION (#PCDATA)>

<!ELEMENT CORRELATION (EXPLOITABILITY?,MALWARE?)>
<!ELEMENT EXPLOITABILITY (EXPLT_SRC)+>
<!ELEMENT EXPLT_SRC (SRC_NAME, EXPLT_LIST)>
<!ELEMENT SRC_NAME (#PCDATA)>
<!ELEMENT EXPLT_LIST (EXPLT)+>
<!ELEMENT EXPLT (REF, DESC, LINK?)>
<!ELEMENT REF (#PCDATA)>
<!ELEMENT DESC (#PCDATA)>
<!ELEMENT LINK (#PCDATA)>
```

```
<!ELEMENT MALWARE (MW_SRC)+>
<!ELEMENT MW_SRC (SRC_NAME, MW_LIST)>
<!ELEMENT MW_LIST (MW_INFO)+>
<!ELEMENT MW_INFO (MW_ID, MW_TYPE?, MW_PLATFORM?, MW_ALIAS?, MW_RATING?,
                   MW_LINK?)>
<!ELEMENT MW_ID (#PCDATA)>
<!ELEMENT MW_TYPE (#PCDATA)>
<!ELEMENT MW_PLATFORM (#PCDATA)>
<!ELEMENT MW_ALIAS (#PCDATA)>
<!ELEMENT MW_RATING (#PCDATA)>
<!ELEMENT MW_LINK (#PCDATA)>

<!ELEMENT RESULT (#PCDATA)>
<!ATTLIST RESULT format CDATA #IMPLIED>

<!-- ============ TICKET INFORMATION  ============== -->

<!ELEMENT TICKETS (OPEN?, RESOLVED?)>
<!ELEMENT OPEN     (SEVERITY_LEVEL_1?, SEVERITY_LEVEL_2?,
                    SEVERITY_LEVEL_3?,
                    SEVERITY_LEVEL_4?, SEVERITY_LEVEL_5?)>
<!ELEMENT RESOLVED (SEVERITY_LEVEL_1?, SEVERITY_LEVEL_2?,
                    SEVERITY_LEVEL_3?,
                    SEVERITY_LEVEL_4?, SEVERITY_LEVEL_5?)>

<!ELEMENT TICKET_NUMBER (#PCDATA)>
```

XPaths for Get Host Information Report

This section describes the XPaths for the get host information report (get_host_info.dtd).

Host — Header Information

The following host information is returned by a **`get_host_info.php`** request.

XPath	element specifications / notes
/HOST	(ERROR | (TRACKING_METHOD, SECURITY_RISK, IP, DNS?, NETBIOS?, OPERATING_SYSTEM?, LAST_SCAN_DATE?, COMMENT?, OWNER?, USER_DEFINED_ATTR_LIST?, USER_LIST?, ASSET_GROUP_LIST?, AUTHENTICATION_RECORD_LIST?, BUSINESS_UNIT_LIST?, VULNS?, POTENTIAL_VULNS?, INFO_GATHERED?, TICKETS?))
/HOST/TRACKING_METHOD	(#PCDATA) The host tracking method assigned to the host. A valid value is “IP address”, “DNS hostname”, or “NetBIOS hostname”.

XPath	element specifications / notes
/HOST/SECURITY_RISK	(#PCDATA)
	The current security risk of the host, reflecting the number of vulnerabilities detected on the host and the relative security risk of those vulnerabilities. Security risk is a value from 1 to 5, where a rating of 5 represents the highest security risk.
/HOST/IP	(#PCDATA)
	The IP address of the host.
/HOST/DNS	(#PCDATA)
	The DNS host name when known.
/HOST/NETBIOS	(#PCDATA)
	The Microsoft Windows NetBIOS host name if appropriate, when known.
/HOST/OPERATING_SYSTEM	(#PCDATA)
	The operating system detected on the host.
/HOST/ERROR	(#PCDATA)
attribute: **number**	**number** is *implied* and if present, will be an error code.

Host — General Information

The host information, described below, is returned by a successful **get_host_info.php** request that includes the **general_info=1** parameter.

XPath	element specifications / notes
/HOST/LAST_SCAN_DATE	(#PCDATA)
	The date and time when the host was last scanned (most recent scan, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/HOST/COMMENT	(#PCDATA)
	User-supplied host comments.
/HOST/OWNER	(USER)
/HOST/OWNER/USER	(FIRSTNAME?, LASTNAME?, USER_LOGIN?)
/HOST/OWNER/USER/FIRSTNAME	(#PCDATA)
	The first name of a user who is the asset owner.
/HOST/OWNER/USER/LASTNAME	(#PCDATA)
	The last name of a user who is the asset owner.
/HOST/OWNER/USER/USER_LOGIN	(#PCDATA)
	The user login name of a user who is the asset owner.
/HOST/USER_LIST	(USER+)
/HOST/USER_LIST/USER/FIRSTNAME	(#PCDATA)
	The first name of a user who has permissions to access the host.
/HOST/USER_LIST/USER/LASTNAME	(#PCDATA)
	The last name of a user who has permission to access the host.

XPath	element specifications / notes
/HOST/USER_LIST/USER/USER_LOGIN (#PCDATA)	
	The user login name of a user who has permission to access the host.
/HOST/USER_DEFINED_ATTR_LIST	
	(USER_DEFINED_ATTR+)
/HOST/USER_DEFINED_ATTR_LIST/USER_DEFINED_ATTR	
	(UDA_INDEX, UDA_TITLE, IDA_VALUE)
/HOST/USER_DEFINED_ATTR_LIST/USER_DEFINED_ATTR/UDA_INDEX (#PCDATA)	
	The index value of the user-defined host attribute.
/HOST/USER_DEFINED_ATTR_LIST/USER_DEFINED_ATTR/UDA_TITLE (#PCDATA)	
	The title of the user-defined host attribute.
/HOST/USER_DEFINED_ATTR_LIST/USER_DEFINED_ATTR/UDA_VALUE (#PCDATA)	
	The value of the user-defined host attribute.
/HOST/ASSET_GROUP_LIST (ASSET_GROUP+)	
/HOST/ASSET_GROUP_LIST/ASSET_GROUP	
	(ASSET_GROUP_TITLE?, CVSS_ENVIRONMENT?)
/HOST/ASSET_GROUP_LIST/ASSET_GROUP_TITLE	
	The title of an asset group that includes the host.
/HOST/ASSET_GROUP_LIST/CVSS_ENVIRONMENT	
	(CVSS_COLLATERAL_DAMAGE_POTENTIAL, CVSS_TARGET_DISTRIBUTION, CVSS_ENV_CR, CVSS_ENV_IR, CVSS_ENV_AR)
/HOST/ASSET_GROUP_LIST/CVSS_ENVIRONMENT/CVSS_COLLATERAL_DAMAGE_POTENTIAL	
	The setting for the CVSS Environmental metric: Collateral Damage Potential as defined for the asset group.
/HOST/ASSET_GROUP_LIST/CVSS_ENVIRONMENT/CVSS_TARGET_DISTRIBUTION	
	The setting for the CVSS Environmental metric: Target Distribution as defined for the asset group.
/HOST/ASSET_GROUP_LIST/CVSS_ENVIRONMENT/CVSS_ENV_CR	
	The setting for the CVSS Environmental metric: Confidentiality Requirement as defined for the asset group.
/HOST/ASSET_GROUP_LIST/CVSS_ENVIRONMENT/CVSS_ENV_IR	
	The setting for the CVSS Environmental metric: Integrity Requirement as defined for the asset group.
/HOST/ASSET_GROUP_LIST/CVSS_ENVIRONMENT/CVSS_ENV_AR	
	The setting for the CVSS Environmental metric: Availability Requirement as defined for the asset group.
/HOST/AUTHENTICATION_RECORD_LIST	
	(AUTH_WINDOWS?, AUTH_UNIX?, AUTH_ORACLE?, AUTH_SNMP?)

XPath	element specifications / notes
/HOST/AUTHENTICATION_RECORD_LIST/AUTH_WINDOWS (#PCDATA)	
	The title of a Windows authentication record that includes the host.
/HOST/AUTHENTICATION_RECORD_LIST/AUTH_UNIX (#PCDATA)	
	The title of a Unix authentication record that includes the host.
/HOST/AUTHENTICATION_RECORD_LIST/AUTH_ORACLE (#PCDATA)	
	The title of an Oracle authentication record that includes the host.
/HOST/AUTHENTICATION_RECORD_LIST/AUTH_SNMP (#PCDATA)	
	The title of an SNMP authentication record that includes the host.
/HOST/BUSINESS_UNIT_LIST	(BUSINESS_UNIT+)
/HOST/BUSINESS_UNIT_LIST/BUSINESS UNIT (#PCDATA)	
	The title of a business unit that includes the host.

Host — Vulnerability Counts

A vulnerability count by severity level list is returned by a successful **`get_host_info.php`** request. Current vulnerabilities that are not fixed are included.

XPath	element specifications / notes
/HOST/VULNS	(SEVERITY_LEVEL_1?, SEVERITY_LEVEL_2?, SEVERITY_LEVEL_3?, SEVERITY_LEVEL_4?, SEVERITY_LEVEL_5?)
/HOST/VULNS/SEVERITY_LEVEL_n (n is a severity level, 1 through 5)	
	(COUNT, (VULNINFO* | TICKET_NUMBER*)
/HOST/VULNS/SEVERITY_LEVEL_n/COUNT	
	The total number of vulnerabilities at each severity level.
/HOST/POTENTIAL_VULNS	(SEVERITY_LEVEL_1?, SEVERITY_LEVEL_2?, SEVERITY_LEVEL_3?, SEVERITY_LEVEL_4?, SEVERITY_LEVEL_5?)
/HOST/POTENTIAL_VULNS/SEVERITY_LEVEL_n (n is a severity level, 1 through 5)	
	(COUNT, (VULNINFO* | TICKET_NUMBER*)
/HOST/POTENTIAL_VULNS/SEVERITY_LEVEL_n/COUNT	
	The total number of potential vulnerabilities at each severity level.
/HOST/INFO_GATHERED	(SEVERITY_LEVEL_1?, SEVERITY_LEVEL_2?, SEVERITY_LEVEL_3?, SEVERITY_LEVEL_4?, SEVERITY_LEVEL_5?)
/HOST/INFO_GATHERED/SEVERITY_LEVEL_n (n is a severity level, 1 through 3)	
	(COUNT, (VULNINFO* | TICKET_NUMBER*)
/HOST/INFO_GATHERED/SEVERITY_LEVEL_n/COUNT	
	The total number of information gathered at each severity level. Qualys assigns severity levels 1 through 3 to information gathered, however users may customize these to assign severity levels 4 and 5.

Host — Vulnerability Information

The host's vulnerability details, described below, are returned by a successful **`get_host_info.php`** request that includes the **`vuln_details=1`** parameter.

XPath	element specifications / notes
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO	
	(QID, SEVERITY_LEVEL, TITLE, VULN_STATUS?, CATEGORY?, PORT?, SERVICE?, PROTOCOL?, INSTANCE?, CVSS_SCORE?, FIRST_FOUND?, LAST_FOUND?, TIMES_FOUND?, VENDOR_REFERENCE_LIST?, CVE_ID_LIST?, BUGTRAQ_ID_LIST?, LAST_UPDATE?, DIAGNOSIS?, DIAGNOSIS_COMMENT?, CONSEQUENCE?, CONSEQUENCE_COMMENT?, SOLUTION?, SOLUTION_COMMENT?, COMPLIANCE?, CORRELATION?, RESULT?)
	"vuln_level" is VULN for a vulnerability, POTENTIAL_VULNS for a potential vulnerability, or INFO_GATHERED for information gathered.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/QID (#PCDATA)	
	The Qualys ID (QID) assigned to the vulnerability, from the Qualys KnowledgeBase.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/SEVERITY_LEVEL (#PCDATA)	
	The severity level assigned to the vulnerability, from the Qualys KnowledgeBase.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/TITLE (#PCDATA)	
	The title of the vulnerability, from the Qualys KnowledgeBase.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/VULN_STATUS (#PCDATA)	
	The vulnerability status. Note: This element not present for information gathered. A valid value is "New" for an active vulnerability that was detected one time, Active for an active vulnerability that was detected at least two times, "Re-Opened" for an active vulnerability that was fixed and then re-opened, and "Fixed" for a vulnerability that was detected previously and is now fixed.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CATEGORY (#PCDATA)	
	The category of the vulnerability.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/PORT (#PCDATA)	
	The port number that the vulnerability was detected on.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/SERVICE (#PCDATA)	
	The service that the vulnerability was detected on.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/PROTOCOL (#PCDATA)	
	The protocol that the vulnerability was detected on.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/INSTANCE (#PCDATA)	
	The Oracle DB instance the vulnerability was detected on.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/FIRST_FOUND (#PCDATA)	
	The date and time when the vulnerability was first detected on the host, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).

XPath	element specifications / notes
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/LAST_FOUND (#PCDATA)	
	The date and time when the vulnerability was last detected on the host (from the most recent scan), in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/TIMES_FOUND (#PCDATA)	
	The total number of times the vulnerability was detected on the host.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/LAST_UPDATE (#PCDATA)	
	The date and time when the vulnerability was last updated in the Qualys KnowledgeBase, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/DIAGNOSIS (#PCDATA)	
	The Qualys provided description of the threat.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/DIAGNOSIS_COMMENT (#PCDATA)	
	User-defined description of the threat, if any.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CONSEQUENCE (#PCDATA)	
	Qualys provided description of the impact.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CONSEQUENCE_COMMENT (#PCDATA)	
	User-provided description of the impact, if any.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/SOLUTION (#PCDATA)	
	Qualys provided description of the solution. When virtual patch information is correlated with a vulnerability, the virtual patch information from Trend Micro appears under the heading “Virtual Patches:”. This includes a list of virtual patches and a link to more information.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/SOLUTION_COMMENT (#PCDATA)	
	User-defined description of the solution, if any.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/COMPLIANCE (COMPLIANCE_INFO+)	
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/COMPLIANCE/COMPLIANCE_INFO	
	(COMPLIANCE_TYPE, COMPLIANCE_SECTION, COMPLIANCE_DESCRIPTION)
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/COMPLIANCE/COMPLIANCE_INFO/ COMPLIANCE_TYPE (#PCDATA)	
	The type of a compliance policy or regulation that is associated with the vulnerability. A valid value is: -HIPAA (Health Insurance Portability and Accountability Act) -GLBA (Gramm-Leach-Bliley Act) -CobIT (Control Objectives for Information and related Technology -SOX (Sarbanes-Oxley Act)
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/COMPLIANCE/COMPLIANCE_INFO/ COMPLIANCE_SECTION (#PCDATA)	
	The section of a compliance policy or regulation associated with the vulnerability.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/COMPLIANCE/COMPLIANCE_INFO/ COMPLIANCE_DESCRIPTION (#PCDATA)	
	The description of a compliance policy or regulation associated with the vulnerability.

XPath	element specifications / notes
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CORRELATION	(EXPLOITABILITY?, MALWARE?)
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CORRELATION/EXPLOITABILITY	(EXPLT_SRC)+
	The <EXPLOITABILITY> element and its sub-elements appear only when there is exploitability information for the vulnerability from third party vendors and/or publicly available sources.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CORRELATION/EXPLOITABILITY/EXPLT_SRC	(SRC_NAME, EXPLT_LIST)
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CORRELATION/EXPLOITABILITY/EXPLT_SRC/SRC_NAME	(#PCDATA)
	The name of a third party vendor or publicly available source of the vulnerability information.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST	(EXPLT)+
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT	(REF, DESC, LINK?)
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/REF	(#PCDATA)
	The CVE reference for the exploitability information.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/DESC	(#PCDATA)
	The description provided by the source of the exploitability information (third party vendor or publicly available source).
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/LINK	(#PCDATA)
	A link to the exploit, when available.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CORRELATION/MALWARE	(MW_SRC)+
	The <MALWARE> element and its sub-elements appear only when there is malware information for the vulnerability from Trend Micro.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CORRELATION/MALWARE/MW_SRC	(SRC_NAME, MW_LIST)
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CORRELATION/MALWARE/MW_SRC/SRC_NAME	(#PCDATA)
	The name of the source of the malware information: Trend Micro.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CORRELATION/MALWARE/MW_SRC/MW_LIST	(MW_INFO)+
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO	(MW_ID, MW_TYPE?, MW_PLATFORM?, MW_ALIAS?, MW_RATING?, MW_LINK?)

XPath	element specifications / notes
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_ID (#PCDATA)	
	The malware name/ID assigned by Trend Micro.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_TYPE (#PCDATA)	
	The type of malware, such as Backdoor, Virus, Worm or Trojan.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_PLATFORM (#PCDATA)	
	A list of the platforms that may be affected by the malware.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_ALIAS (#PCDATA)	
	A list of other names used by different vendors and/or publicly available sources to refer to the same threat.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_RATING (#PCDATA)	
	The overall risk rating as determined by Trend Micro: Low, Medium or High.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_LINK (#PCDATA)	
	A link to malware details.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/RESULT (#PCDATA)	
	Specific scan test results for the vulnerability, from the host assessment data.
attribute: **format**	**format** is *implied* and if present, will be "table," indicating that the results are a table that has columns separated by tabulation characters and rows separated by new-line characters

Host — Vulnerability References

Vulnerability references from sources outside of Qualys are returned by a successful **get_host_info.php** request that includes the **vuln_details=1** parameter when references are available in the Qualys KnowledgeBase.

XPath	element specifications / notes
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/VENDOR_REFERENCE_LIST	
	(VENDOR_REFERENCE+)
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/VENDOR_REFERENCE_LIST/VENDOR_REFERENCE	
	(ID, URL)
	The name of a vendor reference, and the URL to this vendor reference.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/reference_list/reference/ID (#PCDATA)	
	The name of a vendor reference, CVE name, or Bugtraq ID.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/reference_list/reference/URL (#PCDATA)	
	The URL to the vendor reference, CVE name, or Bugtraq ID.

XPath	element specifications / notes
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CVE_ID_LIST (CVE_ID+)	
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CVE_ID_LIST/CVE_ID (ID, URL)	
	A CVE name assigned to the vulnerability, and the URL to this CVE name. CVE (Common Vulnerabilities and Exposures) is a list of common names for publicly known vulnerabilities and exposures. Through open and collaborative discussions, the CVE Editorial Board determines which vulnerabilities or exposures are included in CVE. If the CVE name starts with CAN (candidate) then it is under consideration for entry into CVE.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/BUGTRAQ_LIST (BUGTRAQ_ID+)	
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/BUGTRAQ_LIST/BUGTRAQ_ID (ID, URL)	
	A Bugtraq ID assigned to the vulnerability, and the URL to this Bugtraq ID.

CVSS Scoring Information

CVSS scoring information is returned in the host information report only when CVSS scoring is enabled in the user's account. Specifically, data is returned as follows:

- The CVSS Base and Temporal scores for a particular vulnerability are returned by a successful **`get_host_info.php`** request that includes the **`vuln_details=1`** parameter.
- The CVSS Environmental metrics are returned by a successful **`get_host_info.php`** request that includes the **`general_info=1`** parameter.

The CVSS scoring information returned is described below.

XPath	element specifications / notes
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CVSS_SCORE	
	(CVSS_BASE?, CVSS_TEMPORAL?, CVSS_ENVIRONMENT?)
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CVSS_SCORE/CVSS_BASE	
	(#PCDATA)
	The CVSS Base score defined for the vulnerability.
attribute: **`source`**	Note: This attribute is never returned in XML output for this release.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CVSS_SCORE/CVSS_TEMPORAL	
	(#PCDATA)
	The CVSS Temporal score defined for the vulnerability.
/HOST/vuln_level/SEVERITY_LEVEL_n/COUNT/VULNINFO/CVSS_SCORE/CVSS_ENVIRONMENT	
	(CVSS_COLLATERAL_DAMAGE_POTENTIAL, CVSS_TARGET_DISTRIBUTION, CVSS_ENV_CR, CVSS_ENV_IR, CVSS_ENV_AR)

XPath	element specifications / notes
/HOST/ASSET_GROUP_LIST/CVSS_ENVIRONMENT/CVSS_COLLATERAL_DAMAGE_POTENTIAL (#PCDATA)	
	The setting for the CVSS Environmental metric: Collateral Damage Potential as defined for the asset group.
/HOST/ASSET_GROUP_LIST/CVSS_ENVIRONMENT/CVSS_TARGET_DISTRIBUTION (#PCDATA)	
	The setting for the CVSS Environmental metric: Target Distribution as defined for the asset group.
/HOST/ASSET_GROUP_LIST/CVSS_ENVIRONMENT/CVSS_ENV_CR (#PCDATA)	
	The setting for the CVSS Environmental metric: Confidentiality Requirement as defined for the asset group.
/HOST/ASSET_GROUP_LIST/CVSS_ENVIRONMENT/CVSS_ENV_IR (#PCDATA)	
	The setting for the CVSS Environmental metric: Integrity Requirement as defined for the asset group.
/HOST/ASSET_GROUP_LIST/CVSS_ENVIRONMENT/CVSS_ENV_AR (#PCDATA)	
	The setting for the CVSS Environmental metric: Availability Requirement as defined for the asset group.

Host — Ticket Information

The host's ticket information is returned by a successful **`get_host_info.php`** request. The total number of Open and Resolved tickets at each severity level is reported by default.

When the **`get_host_info.php`** request includes the **`ticket_details=1`** parameter, the host information report lists the ticket numbers at each severity level.

XPath	element specifications / notes
/HOST/TICKETS	(OPEN?, RESOLVED?)
/HOST/TICKETS/OPEN	(SEVERITY_LEVEL_1?, SEVERITY_LEVEL_2?, SEVERITY_LEVEL_3?, SEVERITY_LEVEL_4?, SEVERITY_LEVEL_5?)
/HOST/TICKETS/OPEN/TICKET_NUMBER (#PCDATA)	
	The number of an Open ticket that applies to the host.
/HOST/TICKETS/RESOLVED	(SEVERITY_LEVEL_1?, SEVERITY_LEVEL_2?, SEVERITY_LEVEL_3?, SEVERITY_LEVEL_4?, SEVERITY_LEVEL_5?)
/HOST/TICKETS/RESOLVED/TICKET_NUMBER (#PCDATA)	
	The number of a Resolved ticket that applies to the host.

Ignore Vulnerability Output

The ignore vulnerability output (ignore_vuln_output.dtd) is an XML report returned from the **ignore_vuln.php** function. This report includes a status message and identifies ignored vulnerabilities that were newly defined or removed.

DTD for Ignore Vulnerability Output

A recent DTD for the ignore vulnerability output (ignore_vuln_output.dtd) is shown below.

```
<!-- QUALYS IGNORE VULNERABILITY OUTPUT DTD -->

<!ELEMENT IGNORE_VULN_OUTPUT (API,RETURN)>

<!-- "name" is the name of API -->
<!-- "at" attribute is the current platform date and time -->
<!ELEMENT API (#PCDATA)>
<!ATTLIST API
          name CDATA #REQUIRED
          username CDATA #REQUIRED
          at CDATA #REQUIRED>

<!-- the PCDATA contains an explanation of the status -->
<!ELEMENT RETURN (MESSAGE, IGNORED_LIST?, RESTORED_LIST?)>
<!ATTLIST RETURN
          status (FAILED|SUCCESS|WARNING) #REQUIRED
          number CDATA #IMPLIED>
<!ELEMENT MESSAGE (#PCDATA)*>
<!ELEMENT IGNORED_LIST (IGNORED+)>
<!ELEMENT IGNORED (TICKET_NUMBER, QID, IP, DNS?, NETBIOS?)>
<!ELEMENT TICKET_NUMBER (#PCDATA)>
<!ELEMENT QID (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>

<!ELEMENT RESTORED_LIST (RESTORED+)>
<!ELEMENT RESTORED (TICKET_NUMBER, QID, IP, DNS?, NETBIOS?)>
```

XPaths for Ignore Vulnerability Output

This section describes the XPaths for the ignore vulnerability output (ignore_vuln_output.dtd).

XPath	element specifications / notes
/IGNORE_VULN_OUTPUT	(API, RETURN)
/IGNORE_VULN_OUTPUT/API	(#PCDATA)
attribute: **name**	**name** is *required* and is the API function name.
attribute: **username**	**username** is *required* and is the user login of the API user.
attribute: **at**	**at** is *required* and is the date/time when the function was run in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/IGNORE_VULN_OUTPUT/RETURN	(MESSAGE, IGNORED_LIST?, RESTORED_LIST?)
attribute: **status**	**status** is *required* and is a status code, either SUCCESS, FAILED, or WARNING.
attribute: **number**	**number** is *implied* and, if present, is an error code.
/IGNORE_VULN_OUTPUT/RETURN/MESSAGE	(#PCDATA)
	A descriptive message that corresponds to the status code.
/IGNORE_VULN_OUTPUT/RETURN/IGNORED_LIST	(IGNORED+)
/IGNORE_VULN_OUTPUT/RETURN/IGNORED_LIST/IGNORED	(TICKET_NUMBER, QID, IP, DNS?, NETBIOS?)
/IGNORE_VULN_OUTPUT/RETURN/RESTORED_LIST	(RESTORED+)
/IGNORE_VULN_OUTPUT/RETURN/RESTORED_LIST/RESTORED	(TICKET_NUMBER, QID, IP, DNS?, NETBIOS?)
/IGNORE_VULN_OUTPUT/RETURN/{LIST}/{VULN}/TICKET_NUMBER	(#PCDATA)
	The ticket number related to a vulnerability that was ignored or restored. {LIST} stands for an ignored or restored list. {VULN} stands for an ignored or restored vulnerability.
/IGNORE_VULN_OUTPUT/RETURN/{LIST}/{VULN}/QID	(#PCDATA)
	The QID related to a vulnerability that was ignored or restored. {LIST} stands for an ignored or restored list. {VULN} stands for an ignored or restored vulnerability.
/IGNORE_VULN_OUTPUT/RETURN/{LIST}/{VULN}/IP	(#PCDATA)
	The IP address related to a vulnerability that was ignored or restored. {LIST} stands for an ignored or restored list. {VULN} stands for an ignored or restored vulnerability.
/IGNORE_VULN_OUTPUT/RETURN/{LIST}/{VULN}/DNS	(#PCDATA)
	The DNS host name related to a vulnerability that was ignored or restored. {LIST} stands for an ignored or restored list. {VULN} stands for an ignored or restored vulnerability.
/IGNORE_VULN_OUTPUT/RETURN/{LIST}/{VULN}/NETBIOS	(#PCDATA)
	The NetBIOS host name related to a vulnerability that was ignored or restored. {LIST} stands for an ignored or restored list. {VULN} stands for an ignored or restored vulnerability.

APPENDIX F

User Management Reports

The user management reports provide information about users in a Qualys subscription.

This appendix covers the following topics:

- User Output
- User List Output
- User Action Log Report
- Password Change Output

User Output

The user output is an XML report returned from the **`user.php`** function.

The user output DTD and XPaths are described below.

DTD for User Output

A recent DTD for the user output (user_output.dtd) is shown below.

```
<!-- QUALYS USER OUTPUT DTD -->

<!ELEMENT USER_OUTPUT (API, RETURN, USER?)>

<!-- "name" is the name of API -->
<!-- "at" is the current platform date and time -->
<!ELEMENT API (#PCDATA)>
<!ATTLIST API
          name CDATA #REQUIRED
          username CDATA #REQUIRED
          at CDATA #REQUIRED>

<!-- the PCDATA contains an explanation of the status -->
<!ELEMENT RETURN (MESSAGE?)>
<!ATTLIST RETURN
          status (FAILED|SUCCESS|WARNING) #REQUIRED
          number CDATA #IMPLIED>

<!ELEMENT MESSAGE (#PCDATA)>

<!-- USER element in case password needs to be returned in XML -->
<!ELEMENT USER (USER_LOGIN, PASSWORD)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT PASSWORD (#PCDATA)>
```

XPaths for User Output

This section describes the XPaths for the user output (user_output.dtd).

XPath	element specifications / notes
/USER_OUTPUT (API, RETURN, USER?)	
/USER_OUTPUT/API (#PCDATA)	
attribute: **name**	**name** is *required* and is the API function name.
attribute: **username**	**username** is *required* and is the user login of the API user.
attribute: **at**	**at** is *required* and is the date/time when the function was run in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/USER_OUTPUT/RETURN (MESSAGE?)	
attribute: **status**	**status** is *required* and is a status code, either SUCCESS, FAILED, or WARNING.
attribute: **number**	**number** is *implied* and, if present, is an error code.
/USER_OUTPUT/RETURN/MESSAGE (#PCDATA)	
	A descriptive message that corresponds to the status code.
/USER_OUTPUT/USER (USER_LOGIN, PASSWORD)	
	The USER element (with sub-elements) is returned for a new user account when the user.php request included the send_email=0 input parameter.
/USER_OUTPUT/USER/USER_LOGIN (#PCDATA)	
	The user login ID for the new user account.
/USER_OUTPUT/USER/PASSWORD (#PCDATA)	
	The new and current password for the new user account.

User List Output

The user list is an XML report returned from the **user_list.php** function. This report includes information about users in a subscription.

The user list DTD and XPaths are described below.

DTD for User List Output

A recent DTD for the user list output (user_list_output.dtd) is shown below.

```
<!-- QUALYS USER LIST OUTPUT DTD -->

<!ELEMENT USER_LIST_OUTPUT (ERROR | USER_LIST)>

<!ELEMENT ERROR (#PCDATA)*>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!ELEMENT USER_LIST (USER*)>

<!ELEMENT USER (USER_LOGIN?, EXTERNAL_ID?, CONTACT_INFO,
                ASSIGNED_ASSET_GROUPS?, USER_STATUS, CREATION_DATE,
                LAST_LOGIN_DATE?, USER_ROLE, MANAGER_POC?,
                BUSINESS_UNIT?, UNIT_MANAGER_POC?,
                UI_INTERFACE_STYLE?, PERMISSIONS?, NOTIFICATIONS?)>

<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT EXTERNAL_ID (#PCDATA)>

<!ELEMENT CONTACT_INFO (FIRSTNAME, LASTNAME, TITLE, PHONE, FAX, EMAIL,
                        COMPANY, ADDRESS1, ADDRESS2, CITY, COUNTRY, STATE,
                        ZIP_CODE)>

<!ELEMENT FIRSTNAME (#PCDATA)>
<!ELEMENT LASTNAME (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT PHONE (#PCDATA)>
<!ELEMENT FAX (#PCDATA)>
<!ELEMENT EMAIL (#PCDATA)>
<!ELEMENT COMPANY (#PCDATA)>
<!ELEMENT ADDRESS1 (#PCDATA)>
<!ELEMENT ADDRESS2 (#PCDATA)>
<!ELEMENT CITY (#PCDATA)>
<!ELEMENT COUNTRY (#PCDATA)>
<!ELEMENT STATE (#PCDATA)>
<!ELEMENT ZIP_CODE (#PCDATA)>

<!ELEMENT ASSIGNED_ASSET_GROUPS (ASSET_GROUP_TITLE+)>
```

```
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>

<!ELEMENT USER_STATUS (#PCDATA)>
<!ELEMENT CREATION_DATE (#PCDATA)>
<!ELEMENT LAST_LOGIN_DATE (#PCDATA)>
<!ELEMENT USER_ROLE (#PCDATA)>
<!ELEMENT MANAGER_POC (#PCDATA)>
<!ELEMENT BUSINESS_UNIT (#PCDATA)>
<!ELEMENT UNIT_MANAGER_POC (#PCDATA)>
<!ELEMENT UI_INTERFACE_STYLE (#PCDATA)>

<!ELEMENT PERMISSIONS (CREATE_OPTION_PROFILES, PURGE_INFO, ADD_ASSETS,
                       EDIT_REMEDIATION_POLICY, EDIT_AUTH_RECORDS)>

<!ELEMENT CREATE_OPTION_PROFILES (#PCDATA)>
<!ELEMENT PURGE_INFO (#PCDATA)>
<!ELEMENT ADD_ASSETS (#PCDATA)>
<!ELEMENT EDIT_REMEDIATION_POLICY (#PCDATA)>
<!ELEMENT EDIT_AUTH_RECORDS (#PCDATA)>

<!ELEMENT NOTIFICATIONS (LATEST_VULN, MAP, SCAN, DAILY_TICKETS)>

<!ELEMENT LATEST_VULN (#PCDATA)>

<!ELEMENT MAP (#PCDATA)>
<!ELEMENT SCAN (#PCDATA)>
<!ELEMENT DAILY_TICKETS (#PCDATA)>
```

XPaths for User List Output

This section describes the XPaths for the user list (user_list_output.dtd).

XPath	element specifications / notes
/USER_LIST_OUTPUT	(ERROR | USER_LIST)
/USER_LIST_OUTPUT/ERROR	(#PCDATA)
attribute: **number**	**number** is *implied* and if present, will be an error code.
/USER_LIST_OUTPUT/USER_LIST	(USER*)
/USER_LIST_OUTPUT/USER_LIST/USER	(USER_LOGIN?, EXTERNAL_ID?, CONTACT_INFO, ASSIGNED_ASSET_GROUPS?, USER_STATUS, CREATION_DATE, LAST_LOGIN_DATE?, USER_ROLE, MANAGER_POC?, BUSINESS_UNIT?, UNIT_MANAGER_POC?, UI_INTERFACE_STYLE?, PERMISSIONS?, NOTIFICATIONS?)
/USER_LIST_OUTPUT/USER_LIST/USER/USER_LOGIN	(#PCDATA)
	The Qualys user login ID for the user's account.

XPath	element specifications / notes
/USER_LIST_OUTPUT/USER_LIST/USER/EXTERNAL_ID (#PCDATA)	
	The user's custom external ID, if defined. If not defined, this element does not appear.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO	
	(FIRSTNAME, LASTNAME, TITLE, PHONE, FAX, EMAIL, COMPANY, ADDRESS1, ADDRESS2, CITY, COUNTRY, STATE, ZIP_CODE)
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/FIRSTNAME (#PCDATA)	
	The user's first name.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/LASTNAME (#PCDATA)	
	The user's last name.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/TITLE (#PCDATA)	
	The user's job title.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/PHONE (#PCDATA)	
	The user's phone number.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/FAX (#PCDATA)	
	The user's fax number.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/EMAIL (#PCDATA)	
	The user's email address.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/COMPANY (#PCDATA)	
	The user's company name.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/ADDRESS1 (#PCDATA)	
	The first line of the user's street address.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/ADDRESS2 (#PCDATA)	
	The second line of the user's street address.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/CITY (#PCDATA)	
	The user's city.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/COUNTRY (#PCDATA)	
	The user's country.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/STATE (#PCDATA)	
	The user's state.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/ZIP_CODE (#PCDATA)	
	The zip code of the user's street address.
/USER_LIST_OUTPUT/USER_LIST/USER/ASSIGNED_ASSET_GROUPS (ASSET_GROUP_TITLE+)	
/USER_LIST_OUTPUT/USER_LIST/USER/ASSIGNED_ASSET_GROUPS/ASSET_GROUP_TITLE (#PCDATA)	
	The title of an asset group assigned to the user.
/USER_LIST_OUTPUT/USER_LIST/USER/USER_STATUS (#PCDATA)	
	The user status. Possible values are Active, Inactive and Pending Activation.

XPath	element specifications / notes
/USER_LIST_OUTPUT/USER_LIST/USER/CREATION_DATE (#PCDATA)	
	The date and time when the user account was created.
/USER_LIST_OUTPUT/USER_LIST/USER/LAST_LOGIN_DATE (#PCDATA)	
	The most recent date/time the user logged into Qualys using the user login ID specified in the <USER_LOGIN> element. This element is returned when the API request was made by a Manager or Unit Manager. For a Manager, the last login date is returned for all users in the subscription. For a Unit Manager, the last login date is returned for users in the Unit Manager's same business unit.
/USER_LIST_OUTPUT/USER_LIST/USER/USER_ROLE (#PCDATA)	
	The user role assigned to the user. Possible values are Manager, Unit Manager, Scanner, Reader and Contact.
/USER_LIST_OUTPUT/USER_LIST/USER/MANAGER_POC (#PCDATA)	
	A flag indicating whether the user is the Manager Point of Contact (POC) for the subscription. The value 1 is returned when this user is the Manager POC. The value 0 is returned when this user is not the Manager POC.
/USER_LIST_OUTPUT/USER_LIST/USER/BUSINESS_UNIT (#PCDATA)	
	The business unit the user belongs to. If the user is not part of a business unit then the value is "Unassigned".
/USER_LIST_OUTPUT/USER_LIST/USER/UNIT_MANAGER_POC (#PCDATA)	
	A flag indicating whether this user is the Unit Manager Point of Contact (POC) for the user's business unit. The value 1 is returned when this user is the Unit Manager POC. The value 0 is returned when this user is not the Unit Manager POC.
/USER_LIST_OUTPUT/USER_LIST/USER/UI_INTERFACE_STYLE (#PCDATA)	
	The user interface style applied to the user account. Possible values are standard_blue, navy_blue, coral_red, olive_green and accessible_high_contrast.
/USER_LIST_OUTPUT/USER_LIST/USER/PERMISSIONS	
	(CREATE_OPTION_PROFILES, PURGE_INFO, ADD_ASSETS, EDIT_REMEDIATION_POLICY, EDIT_AUTH_RECORDS)
/USER_LIST_OUTPUT/USER_LIST/USER/PERMISSIONS/CREATE_OPTION_PROFILES (#PCDATA)	
	A flag indicating whether the user is granted permission to create personal option profiles. The value 1 is returned when the user is granted this permission. The value 0 is returned when the user is not granted this permission.
/USER_LIST_OUTPUT/USER_LIST/USER/PERMISSIONS/PURGE_INFO (#PCDATA)	
	A flag indicating whether the user is granted permission to permanently delete saved host information. The value 1 is returned when the user is granted this permission. The value 0 is returned when the user is not granted this permission.
/USER_LIST_OUTPUT/USER_LIST/USER/PERMISSIONS/ADD_ASSETS (#PCDATA)	
	A flag indicating whether the Unit Manager is granted permission to add IPs and domains to the user's business unit, and thus to the subscription. The value 1 is returned when the user is granted this permission. The value 0 is returned when the user is not granted this permission.

XPath	element specifications / notes
/USER_LIST_OUTPUT/USER_LIST/USER/PERMISSIONS/EDIT_REMEDIATION_POLICY (#PCDATA)	
	A flag indicating whether the Unit Manager is granted permission to create and edit a remediation policy for the user's business unit. The value 1 is returned when the user is granted this permission. The value 0 is returned when the user is not granted this permission.
/USER_LIST_OUTPUT/USER_LIST/USER/PERMISSIONS/EDIT_AUTH_RECORDS (#PCDATA)	
	A flag indicating whether the Unit Manager is granted permission to create and edit authentication records when all of the target hosts in the record are in the user's business unit. The value 1 is returned when the user is granted this permission. The value 0 is returned when the user is not granted this permission.
/USER_LIST_OUTPUT/USER_LIST/USER/NOTIFICATIONS (LATEST_VULN, MAP, SCAN, DAILY_TICKETS)	
/USER_LIST_OUTPUT/USER_LIST/USER/NOTIFICATIONS/LATEST_VULN (#PCDATA)	
	A flag indicating how often the user receives the Latest Vulnerabilities email notification. Possible values are weekly, daily and none.
/USER_LIST_OUTPUT/USER_LIST/USER/NOTIFICATIONS/MAP (#PCDATA)	
	A flag indicating whether the user receives the Map Notification via email. The value will be one of: "ags" - the user receives the Map Notification (this option is set to "On" in the UI) "none" - the user does not receive the Map Notification (this option is set to "Off" in the UI)
/USER_LIST_OUTPUT/USER_LIST/USER/NOTIFICATIONS/SCAN (#PCDATA)	
	A flag indicating whether the user receives the Scan Summary Notification via email. The value will be one of: "ags" - the user receives the Scan Summary Notification (this option is set to "On" in the UI) "none" - the user does not receive the Scan Summary Notification (this option is set to "Off" in the UI)
/USER_LIST_OUTPUT/USER_LIST/USER/NOTIFICATIONS/DAILY_TICKETS (#PCDATA)	
	A flag indicating whether the user receives the Daily Trouble Tickets Updates email notification. The value 1 is returned when this notification should be sent to the user. The value 0 is returned when this notification should not be sent to the user.

User Action Log Report

The action log report is an XML report returned from the **`action_log_report.php`** function. This report includes information about actions performed by users in the subscription.

The action log report DTD and XPaths are described below.

DTD for Action Log Report

A recent DTD for the action log report (action_log_report.dtd) is shown below.

```
<!-- QUALYS ACTION LOG REPORT DTD -->

<!ELEMENT ACTION_LOG_REPORT (ERROR | (DATE_FROM, DATE_TO, USER_LOGIN?,
                             ACTION_LOG_LIST))>

<!ELEMENT ERROR (#PCDATA)*>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!ELEMENT DATE_FROM (#PCDATA)*>
<!ELEMENT DATE_TO (#PCDATA)*>
<!ELEMENT USER_LOGIN (#PCDATA)*>

<!ELEMENT ACTION_LOG_LIST (ACTION_LOG)*>
<!ELEMENT ACTION_LOG (DATE, MODULE, ACTION, DETAILS, USER, IP?)>
<!ELEMENT DATE (#PCDATA)>
<!ELEMENT MODULE (#PCDATA)>
<!ELEMENT ACTION (#PCDATA)>
<!ELEMENT DETAILS (#PCDATA)>

<!ELEMENT USER (USER_LOGIN, FIRSTNAME, LASTNAME, ROLE)>
<!ELEMENT FIRSTNAME (#PCDATA)>
<!ELEMENT LASTNAME (#PCDATA)>
<!ELEMENT ROLE (#PCDATA)>

<!ELEMENT IP (#PCDATA)>
```

XPaths for Action Log Report

This section describes the XPaths for the action log report (action_log_report.dtd).

XPath	element specifications / notes
/ACTION_LOG_REPORT	(ERROR | (DATE_FROM, DATE_TO, USER_LOGIN?, ACTION_LOG_LIST))
/ACTION_LOG_REPORT/ERROR	(#PCDATA)
attribute: **`number`**	**`number`** is *implied* and if present, will be an error code.

XPath	element specifications / notes
/ACTION_LOG_REPORT/DATE_FROM (#PCDATA)	
	The start date and time of the time window for downloading action log entries, in YYYY-MMDDTHH:MM:SSZ format (UTC/GMT). Note: If the time is not specified as part of the "date_from" input parameter for the action log request, then the time is set to the start of the day: T00:00:00Z
/ACTION_LOG_REPORT/DATE_TO (#PCDATA)	
	The end date and time of the time window for downloading action log entries, in YYYY-MMDDTHH:MM:SSZ format (UTC/GMT). Note: If the "date_to" input parameter is not specified for the action log request, then the current date and time are used. If the date is specified but the time is not specified, then the time is set to the end of the day: T23:59:59Z
/ACTION_LOG_REPORT/USER_LOGIN (#PCDATA)	
	The Qualys user login ID specified to filter results. Note: This element appears only when the "user_login" input parameter is specified for the action log request.
/ACTION_LOG_REPORT/ACTION_LOG_LIST (ACTION_LOG)*	
/ACTION_LOG_REPORT/ACTION_LOG_LIST/ACTION_LOG	
	(DATE, MODULE, ACTION, DETAILS, USER, IP?)
/ACTION_LOG_REPORT/ACTION_LOG_LIST/ACTION_LOG/DATE (#PCDATA)	
	The date and time when the action occurred, in YYYY-MMDDTHH:MM:SSZ format (UTC/GMT).
/ACTION_LOG_REPORT/ACTION_LOG_LIST/ACTION_LOG/MODULE (#PCDATA)	
	The module affected by the action. See the Qualys online help for a listing.
/ACTION_LOG_REPORT/ACTION_LOG_LIST/ACTION_LOG/ACTION (#PCDATA)	
	The action performed. See the Qualys online help for a listing.
/ACTION_LOG_REPORT/ACTION_LOG_LIST/ACTION_LOG/DETAILS (#PCDATA)	
	Additional information about the action. For example, details may include map and scan targets, scan reference numbers and specific changes to account configurations.
/ACTION_LOG_REPORT/ACTION_LOG_LIST/ACTION_LOG/USER	
	(USER_LOGIN, FIRSTNAME, LASTNAME, ROLE)
/ACTION_LOG_REPORT/ACTION_LOG_LIST/ACTION_LOG/USER/USER_LOGIN (#PCDATA)	
	The Qualys user login ID for the user who performed the action.
/ACTION_LOG_REPORT/ACTION_LOG_LIST/ACTION_LOG/USER/FIRSTNAME (#PCDATA)	
	The first name of the user who performed the action.
/ACTION_LOG_REPORT/ACTION_LOG_LIST/ACTION_LOG/USER/LASTNAME (#PCDATA)	
	The last name of the user who performed the action.
/ACTION_LOG_REPORT/ACTION_LOG_LIST/ACTION_LOG/USER/ROLE (#PCDATA)	
	The user role (Manager, Unit Manager, Scanner or Reader) assigned to the user who performed the action.
/ACTION_LOG_REPORT/ACTION_LOG_LIST/ACTION_LOG/IP (#PCDATA)	
	The IP address of the system used by the user to perform the action.

Password Change Output

The password change output is an XML report returned from the **`password_change.php`** function. This report identifies whether passwords were changed for user accounts.

The password change report DTD and XPaths are described below.

DTD for Password Change Report

A recent DTD for the password change output (password_change_output.dtd) is shown below.

```
<!-- QUALYS PASSWORD CHANGE OUTPUT DTD -->

<!ELEMENT PASSWORD_CHANGE_OUTPUT (API,RETURN)>

<!-- "name" is the name of API -->
<!-- "at" attribute is the current platform date and time -->
<!ELEMENT API (#PCDATA)>
<!ATTLIST API
          name CDATA #REQUIRED
          username CDATA #REQUIRED
          at CDATA #REQUIRED>

<!-- the PCDATA contains an explanation of the status -->
<!ELEMENT RETURN (MESSAGE, CHANGES?, NO_CHANGES?)>
<!ATTLIST RETURN
          status (FAILED|SUCCESS|WARNING) #REQUIRED
          number CDATA #IMPLIED>
<!ELEMENT MESSAGE (#PCDATA)*>

<!ELEMENT CHANGES (USER_LIST)>
<!ATTLIST CHANGES count CDATA #IMPLIED>
<!ELEMENT USER_LIST (USER+)>
<!ELEMENT USER (USER_LOGIN, PASSWORD?, REASON?)>

<!ELEMENT NO_CHANGES (USER_LIST)>
<!ATTLIST NO_CHANGES count CDATA #IMPLIED>
```

XPaths for Password Change Report

This section describes the XPaths for the password change output (password_change_output.dtd).

XPath	element specifications / notes
/PASSWORD_CHANGE_OUTPUT	(API, RETURN)
/PASSWORD_CHANGE_OUTPUT/API	(#PCDATA)
attribute: **name**	**name** is *required* and is the API function name.
attribute: **username**	**username** is *required* and is the user login of the API user.
attribute: **at**	**at** is *required* and is the date/time when the function was run in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/PASSWORD_CHANGE_OUTPUT/RETURN	(MESSAGE, CHANGES?, NO_CHANGES?)
attribute: **status**	**status** is *required* and is a status code, either SUCCESS, FAILED, or WARNING.
attribute: **number**	**number** is *implied* and, if present, is an error code.
/PASSWORD_CHANGE_OUTPUT/RETURN/MESSAGE	(#PCDATA)
	A descriptive message that corresponds to the status code.
/PASSWORD_CHANGE_OUTPUT/RETURN/CHANGES	(USER_LIST)
attribute: **count**	**count** is *implied* and, if present, is the total number of user accounts for which passwords were updated.
/PASSWORD_CHANGE_OUTPUT/RETURN/CHANGES/USER_LIST	(USER+)
/PASSWORD_CHANGE_OUTPUT/RETURN/CHANGES/USER_LIST/USER	(USER_LOGIN, PASSWORD?, REASON?)
	The USER element (with sub-elements) is returned for a user account when the password_change.php request included the email=0 input parameter.
/PASSWORD_CHANGE_OUTPUT/RETURN/CHANGES/USER_LIST/USER/USER_LOGIN	(#PCDATA)
	The user login ID for a user account.
/PASSWORD_CHANGE_OUTPUT/RETURN/CHANGES/USER_LIST/USER/PASSWORD	(#PCDATA)
	The new and current password for the user account.
/PASSWORD_CHANGE_OUTPUT/RETURN/CHANGES/USER_LIST/USER/REASON	(#PCDATA)
	The reason why the password for the user account was not updated. For example, if the user has running maps and/or scans.
/PASSWORD_CHANGE_OUTPUT/RETURN/NO_CHANGES	(USER_LIST)
attribute: **count**	**count** is *implied* and, if present, is the total number of user accounts which do not have changed passwords.
/PASSWORD_CHANGE_OUTPUT/RETURN/NO_CHANGES/USER_LIST	(USER+)

APPENDIX G

Error Codes

The Qualys API functions return numeric error codes that are grouped by category. This appendix identifies the error categories and the individual error codes they contain.

Each Qualys API function can return errors from multiple categories. There are error categories for authentication, maps, scans, scheduled scans, reports, management functions like report list and report delete, and input parameters like IP addresses and domains.

Applications should standardize on numeric error codes, not the error message text, since the numeric codes remain constant from release to release of the Qualys API.

Error Codes by Category

This section describes the error codes listed by category.

Error code range	Category / Error codes
1000 - 1999	Maintenance Errors
	Generic
	1900 ..... Invalid option on url line
	1901 ..... Unknown parameter "<parameter>"
	1902 ..... Missing targets. You must have entered a domain or have domains in an entered asset group.
	1903 ..... Missing value for "<parameter>"
	1904 ..... Invalid/unknown parameter "<parameter>"
	1905 ..... Invalid value for "<parameter>"
	1906 ..... Invalid value for "<parameter>". Maximum text length exceeded.
	1960 ..... The configured maximum number of API instances are already running
	1965 ..... The configured maximum number of API calls have already been made in the configured time period
	1999 ..... Generic maintenance error
2000 - 2999	Authentication Errors
	User-produced errors
	2000 ..... Invalid login/password
	2001 ..... Account expired
	2002 ..... Account inactive
	2003 ..... Has not accepted EULA
	2004 ..... Account locked: recrypting reports
	2005 ..... Account used is not enabled for use with a Scanner Appliance
	2006 ..... Only Enterprise accounts can use the MSP API
	2007 ..... Client IP is not in the list of secure IPs
	2008 ..... This account has been locked after too many unsuccessful login attempts
	2009 ..... Password has expired
	2010 ..... User account is not authorized to perform this function
	2011..... Two factor authentication requirement for this account prevents access to the MSP API
	Platform-produced errors
	2500 ..... Service level does not exist
	Generic
	2999 ..... Generic authentication error

Error code range	Category / Error codes
3000 - 3999	Scan Errors
	User-produced errors
	3000 ..... No IP address submitted 3001 ..... Missing Scanner Appliance name 3002 ..... Invalid Scanner Appliance name 3003 ..... Non-authorized IPs found in target 3004 ..... Maximum number of scans per IP exceeded 3005 ..... Maximum number of scans exceeded 3006 ..... Service level does not allow scanning 3007 ..... Maximum concurrent scan limit reached 3009 ..... Too many IP addresses (pay per scan) 3010 ..... Too many IP scans (pay per scan) 3011..... Invalid list of vulnids 3012 ..... Too many vulnids specified 3013 ..... Two lists of vulnids specified 3014 ..... Invalid option “<profile title>”. Expecting one of... 3015 ..... The option profile “<title>” enables runtime vulnerability selection, and this feature is not supported using the API 3016 ..... Private use network IP addresses can only be scanned or mapped using a scanner appliance. Please either select another target or select a scanner appliance for this task. 3017 ..... You have chosen specific_vulns: <vulnids>. The option profile <title> has <profile option> selected which is incompatible with using specific_vulns.
	Platform-produced errors
	3500 ..... Unable to determine scanner version 3501 ..... Unable to determine vulnerability signatures version 3502 ..... No output 3503 ..... No report reference returned 3504 ..... No end of scan returned 3505 ..... No number of hosts returned 3506 ..... Thread still running 3507 ..... Modules still running 3508 ..... Scan cancelled 3509 ..... No hosts alive 3510 ..... Save error while storing report 3511..... Unable to save report data because the scan did not complete 3512 ..... Internal web server error (orchestrators not responding)
	Generic
	3999 ..... Generic scan error

Error code range	Category / Error codes
4000 - 4999	Map Errors
	User-produced errors
	4000 ..... No target supplied
	4001 ..... Domain not in account
	4002 ..... Netblock not in account
	4003 ..... Service level does not allow discovery (mapping)
	4004 ..... Maximum concurrent map limit exceeded
	4005 ..... Missing Scanner Appliance name
	4006 ..... Invalid Scanner Appliance name
	4007 ..... Private use network IP addresses can only be scanned or mapped using a scanner appliance. Please either select another target or select a scanner appliance for this task.
	Platform-produced errors
	4500 ..... Unable to determine scanner version
	4501 ..... Unable to determine vulnerability signatures package version
	4502 ..... Map cancelled
	4503 ..... No hosts found
	Generic
	4999 ..... Generic map error

Error code range	Category / Error codes
5000 - 5999	IP and Get Host Info Errors
	User-produced errors
	5000 ..... Invalid IP or range
	5001 ..... Loopback not allowed
	5002 ..... IP in reverse order
	5003 ..... Multiple class A networks are not allowed
	5004 ..... Duplicate start of range
	5005 ..... Duplicate end of range
	5006 ..... IP range intersection
	5007 ..... IP range inside another range
	5008 ..... Single IP in netblock
	5009 ..... Same start and end
	5010 ..... No parameter given for “host_ip”, “host_dns”, or “host_netbios”
	5011..... You must specify only one “host_ip”, “host_dns”, or “host_netbios”
	5012 ..... Invalid subnet mask
	5013 ..... More than one host found for the specified host_ip|host_dns|host_netbios
	5014 ..... Invalid syntax for the specified IP
	5015 ..... Bad DNS host name specified
	5016 ..... Bad NetBIOS host name specified
	5017 ..... Invalid vuln_severity specified
	5018 ..... Invalid potential_vuln_severity specified
	5019 ..... Invalid ig_severity specified
	5020 ..... Invalid general_info value specified
	5021 ..... Invalid vuln_details value specified
	5022 ..... Invalid ticket_details value specified
	5023 ..... Maximum allowed length for field exceeded
	5024 ..... Maximum allowed length for comment field exceeded
	5025 ..... Invalid user account specified
	5101 ..... Invalid “<parameter>”. IPs do not exist in the user account.
	5102 ..... Invalid “<parameter>”: invalid target IPs (invalid subnet mask)
	Generic
	5999 ..... Generic IP error
6000 - 6999	Domain Errors
	User-produced errors
	6000 ..... Domain not RFC compliant (invalid domain)
	6001 ..... Cannot start with www
	6002 ..... Invalid value for “<parameter>”: <domains>. Cannot add or delete domains which are not in the subscription.
	Generic
	6999 ..... Generic domain error

Error code range	Category / Error codes
7000 - 7999	Report Errors
	User-produced errors
	7000 ..... Missing reference code for map or scan 7001 ..... Invalid reference code for map or scan 7003 ..... No report with this reference code 7004 ..... Scan or map is running 7005 ..... No host alive (an empty scan report was saved since the scan didn't find any target hosts alive)
	Generic
	7999 ..... Generic reference error
8000 - 8999	Scan Report Errors
	Platform-produced errors
	8500 ..... Scan currently running
	Generic
	8999 ..... Generic scan report error
9000 - 9999	Scan Report List Errors
	Generic
	9999 ..... Generic scan report list error
10000 - 10999	Scan Report Delete Errors
	Generic
	10999 ..... Generic scan report delete error
11000 - 11999	Scan Running List Errors
	Platform-produced errors
	11000..... No scan or map running
	Generic
	11999..... Generic scan running error
12000 - 12999	Map Report List Errors
	Generic
	12999 ..... Generic map report list error
13000 - 13999	Map Report Delete Errors
	Generic
	13999 ..... Generic map report delete error

Error code range	Category / Error codes
14000 - 14999	Scheduled Task Errors
	User-produced errors
	14000 ..... A scheduled task with this name already exists 14001 ..... Too many scheduled tasks 14002 ..... Missing Day of Week 14003 ..... Missing Day of Month 14004 ..... This task does not exist or you don't have permissions to delete it 14005 ..... The option profile "<title>" enables runtime vulnerability selection, and this feature is not supported using the API 14010 ..... Either Time Zone code or Time Zone parameter must be specified 14011..... Time zone code does not match the list from the schedule_scan_time_zones.php API 14012 ..... Cannot specify gmt shift -7 together with time zone code US-CA and/or DST 14013 ..... Specified time zone code does not support DST
	Generic
	14999 ..... Generic scheduled task error
15000 - 15999	Scan Cancel Errors
	User-produced errors
	15000 ..... No running scan with this reference
	Platform-produced errors
	15500..... Internal error
	Generic
	15999 ..... Generic scan cancel error

Error code range	Category / Error codes
17000 - 17999	Remediation Ticket Errors
	User-produced errors
	17000 ..... Invalid value for “<parameter>”. Date is invalid.
	17001 ..... Invalid value for “states”. Must contain only valid values: OPEN, RESOLVED, CLOSED, IGNORED.
	17002 ..... Invalid value for “<parameter>”. Must contain only valid ticket numbers or ranges.
	17003 ..... You must supply a value for “ticket_numbers” or “since” date.
	17004 ..... Specified too many tickets to <edit or delete> all at once (limit is 20,000)
	17006 ..... Value of “vuln_details” is invalid
	17007 ..... Invalid value for “<parameter>” (vuln_severities or potential_vuln_severities). Valid value is: 1, 2, 3, 4, 5.
	17008 ..... Invalid value for “overdue”. Valid value is: 0, 1.
	17009 ..... Invalid value for “<parameter>”. The user is not an active, assignable user in your subscription.
	17010 ..... Invalid value for “qids”. Too many QIDs (maximum is 10).
	17011..... XML parsing error: error message from PHP4 XML parsing engine
18000 - 18999	Asset Group Errors
	User-produced errors
	18000 ..... Invalid value for “<parameter>”: <title>.
	18001 ..... Invalid value for “<parameter>”: <title>. User not authorized to view/delete asset group.
	18003 ..... Asset group has no IPs
	18005 ..... Invalid value for “<parameter>”: All. This title is reserved by the service. Please use a different title.
	18006 ..... Invalid value for “<parameter>”: <title>. Asset group title does not exist.
	18007 ..... Invalid value for “<title>”. Asset group title already exists.
	Generic
	18999 ..... Generic asset group error
19000 - 19999	Option Profile Errors
	User-produced errors
	19001 ..... Invalid option profile name “<title>”. Expecting one of...
	19002 ..... Bandwidth impact no longer supported
	19003 ..... Missing value for “<parameter>”.
	19005 ..... Invalid value for “<parameter>”.
	19006 ..... Invalid value for “<parameter>”. Value is longer than <n> characters.

Error code range	Category / Error codes
20000 - 20999	Scanner Appliance Errors
	User-produced errors
	20000 ..... Default Scanner Appliance requested, no iscanner_name allowed
	20001 ..... This account has no active Scanner Appliance. Please contact your administrator if you think this is an error.
	20002 ..... The default scanner for the asset group "<title>" is no longer valid. Please see your administrator or add a new default scanner to the asset group.
	20999 ..... Invalid scanner appliances: not assigned to this subscription
21000 - 21999	Account Errors
	User-produced errors
	21000 ..... There are already 100 accounts with the same contact information. Please enter a different first name and/or last name.
22000 - 22999	KnowledgeBase Errors
	User-produced errors
	22000 ..... QID does not exist
	22001 ..... Not authorized to download knowledgebase
23000 - 23999	Subscription Errors
	User-produced errors
	23003 ..... The tracking method cannot be applied because the host name is not known for one or more hosts.
	23004 ..... Duplicate entries found for tracking method. Please use the Qualys user interface to change tracking method.
	23009 ..... The number of purchased IPs has been exceeded
	23012 ..... IP does not exist in the subscription
	23013 ..... IP exists in the subscription

Error code range	Category / Error codes
24000 - 24999	Account Configuration Errors
	User-produced errors
	24000 ..... Invalid “<parameter>”: CVSS scoring not enabled
	24100 ..... Invalid value for “<parameter>”: <template ID>. Report template does not exist.
	24101 ..... Invalid value for “parameter”: <template ID>. User account not authorized to run template.
	24103 ..... Invalid value for “parameter”: <template ID>. Report template type is not automatic.
	24104 ..... No target hosts are defined for “<parameter>”: <template ID>. Missing target asset groups.
	24200 ..... Invalid value for “<parameter>”: <prefix:value>. Valid prefix value is: begin, match, contain, or end.
	24201 ..... Invalid value for “tracking_method”. Valid value is: ip, dns, or netbios.
	24202 ..... Invalid value for “host_os”: <prefix:string>. Operating system name does not match available names.
	24203 ..... Invalid value for “vuln_service”: <value>. Unknown service name.
	24204 ..... Invalid value for “qids”: -1. QID (Qualys ID) must be an integer in range 0-999999.
	24250 ..... Asset search result set truncated at 15,001 records.
	24500 ..... Invalid value for “<parameter1>” and “<parameter2>”. Dates are in reverse order. Please switch start and end dates.
	24501 ..... Invalid value for “<parameter1>” and “<parameter2>”. Date range must not exceed 12 months. Please reduce the date range.

INDEX

A

`acceptEULA.php` function 194
action log report
    DTD 375
    XPath elements 375
action log report DTD 203
`action_log_report.php` function 201
API conventions 14
API limits 17
asset data report
    DTD 142, 298
    request 139
    XPath elements 302
asset domain list
    DTD 123, 282
    XPath elements 282
asset group list
    DTD 132, 283
    XPath elements 276, 284
asset groups 29, 32, 62, 89, 135, 144
asset IP list
    DTD 119, 278
    XPath elements 279
asset management functions
    `asset_data_report.php` 139
    `asset_domain_list.php` 123
    `asset_domain.php` 120
    `asset_group_delete.php` 133
    `asset_group_list.php` 132
    `asset_group.php` 124
    `asset_ip_list.php` 118
    `asset_ip.php` 112
    `asset_range_info.php` 143
    `asset_search.php` 134
    `report_template_list.php` 140
    summary of functions 108
asset range info report
    DTD 144, 294
    request 143
asset search report
    DTD 138, 287
    XPath elements 289
asset search request 134
`asset_data_report.php` function 139
`asset_domain_list.php` function 123
`asset_domain.php` function 120
`asset_group_delete.php` function 133
`asset_group_list.php` function 132
`asset_group.php` function 124
`asset_groups` parameter 29, 62, 89, 135, 144
`asset_ip_list.php` function 118
`asset_ip.php` function 112
`asset_range_info.php` function 143
`asset_search.php` function 134
authentication 13, 14
automatic scan data 110

C

cancel a running map 74
cancel a running scan 36
characters in URLs 15
compliance information 219, 241, 311, 360
country codes 189
custom ports 102
CVE 218
CVSS Scoring 125, 218

D

date format 15
dead hosts 101
default ports 102
default scanner 29, 33, 62, 66, 90
`default_scanner` parameter 29, 62, 90
delete a saved map report 80
delete a saved scan report 42
discovery 10, 53, 54

domain names
map requests 65, 71
none domain 57
domain parameter 62, 71
domain_list.php function 105
DTDs for reports
action log report 203
asset data report 142
asset domain list 123
asset group list 132
asset IP list 119
asset range info report 144
asset search report 138
host information report 173
ignore vulnerability output 177
KnowledgeBase download output 51
map report 68, 72
map report list 77
password change output 206
running scans and maps list 35, 73
scan options report 102
scan report 34
scan report list 39
scan target history output 48
scanner appliance list 103
scheduled scans report 99
ticket delete output 162
ticket edit output 160
ticket information report 168
ticket list deleted output 165
ticket list output 157
user list output 200
user output 192, 197
DTDs, most recent 13

E

email notification 31, 63
error codes 379
external scanners 32, 66

F

function name
action_log_report.php 201
asset_data_report.php 139
asset_domain_list.php 123
asset_domain.php 120
asset_group_delete.php 133
asset_group_list.php 132
asset_group.php 124
asset_ip_list.php 118
asset_ip.php 112
asset_range_info.php 143
asset_search.php 134
get_host_info.php 170
get_tickets.php 166
ignore_vuln.php 174
iscanner_list.php 103
knowledgebase_download.php 49
map_report_list.php 76
map_report.php 78
map.php 69
map-2.php 60
password_change.php 204
report_template_list.php 140
scan_cancel.php 36, 74
scan_options.php 100
scan_report_delete.php 42, 80
scan_report_list.php 38
scan_report.php 40
scan_running_list.php 35, 73
scan_target_history.php 44
scan.php 27
scheduled_scans.php 86
ticket_delete.php 161
ticket_edit.php 158
ticket_list_deleted.php 163
ticket_list.php 155
time_zone_code_list.php 95
user_list.php 198
user.php 182, 194, 196

function suite
asset management 108
network discovery (map) 58
preferences 84
remediation management 150, 169
security audit (scan) 25
user management 181

G

GET method 14
`get_host_info.php` function 170
`get_tickets.php` function 166
`group_list.php` function 106

H

host information function
`get_host_info.php` 170
host information report
DTD 173, 351
XPath elements 355
host remediation functions 169
host scan data 110
host target 31, 32
host tracking method 111, 112

I

ignore vulnerability output
DTD 177, 365
XPath elements 366
`ignore_vuln.php` function 174
invalid tickets 153
IP addresses 31, 32
IP ranges 31
`ip_list.php` function 104
`iscanner_list.php` function 103
`iscanner_name` parameter 29, 62, 89

K

keep alive line 28, 61, 69
KnowledgeBase download 49
KnowledgeBase download output
DTD 51
XPath elements 239
knowledgebase download output
DTD 236
`knowledgebase_download.php` function 49

L

load balancer check 101

M

map functions
`asset_domain_list.php` 123
`asset_group_list.php` 132
cancel a running map 74
delete a saved map report 80
list running maps 73
`map_report_list.php` 76
`map_report.php` 78
`map.php` 69
`map-2.php` 60
overview 10, 54
`scan_cancel.php` 74
`scan_report_delete.php` 80
`scan_running_list.php` 73
summary of functions 58
map report
DTD 68, 72, 79, 246, 252
internal network 54
network perimeter 54
XPath elements 248, 254
map report list 76
DTD 77, 257
XPath elements 258
map request 60, 69
map summary notification 63
`map_report_list.php` function 76
`map_report.php` function 78
`map.php` function 69
`map-2.php` function 60

N

NAC option, scanner appliance 274
NAM option, scanner appliance 274
netblocks 56
network discovery 10, 53, 54
network IP address blocks 56
network security audits 10, 21
ng 219

O

`option` parameter 30, 63, 90
option profile 22, 55, 213, 248, 254
overdue tickets 153

P

password change output
- DTD 377
- XPath elements 378

password change output DTD 206
`password_change.php` function 204
PCI flag in scan report 219
ports
- custom list 102
- default 102
- full 102
- range 102

ports to scan 101, 102
POST method 14
preferences functions
- `iscanner_list.php` 103
- `scan_options.php` 100
- `scheduled_scans.php` 86
- summary of functions 84

profile 22, 55, 213, 248, 254

Q

Qualys
- API server 14
- network discovery 53
- network security audits 21
- reporting 207, 245
- user account 13

Qualys API server 14
Qualys End User Agreement (EULA) 194
Qualys EULA 194
Qualys platform 12
Qualys Support 7
Qualys user account 13
Qualys user interface 83

R

range of IP addresses 31
remediation management functions
- `get_tickets.php` 166
- `ignore_vuln.php` 174
- summary of functions 150, 169
- `ticket_delete.php` 161
- `ticket_edit.php` 158
- `ticket_list_deleted.php` 163
- `ticket_list.php` 155

report DTDs, most recent 13
report template ID 140
report template list 140
`report_template_list.php` function 140

reports
action log report 203, 375
asset data report 142, 298
asset domain list 123, 282
asset group list 132, 283
asset IP list 119, 278
asset range info report 144, 294
asset search report 138, 287
date format 15
decoding reports 13
host information report 173
ignore vulnerability output 177
KnowledgeBase download output 51, 236
map report 68, 72, 79
map report list 77, 257
password change output 206, 377
running scans and maps list 35, 73, 228
scan options report 102
scan report 34, 41, 208
scan report list 39, 225
scan target history output 48, 231
scanner appliance list 103, 273
scheduled scans report 99
scheduled tasks report 262
ticket delete output 162
ticket edit output 160
ticket information report 168
ticket list deleted output 165
ticket list output 157
time zone code list 96
user list output 200, 370
user output 192, 197, 368
running maps 73, 74
running scans 35, 36
running scans and maps 35, 73
running scans and maps list
DTD 35, 73, 228
XPath elements 229

S

save_report parameter 31, 63
saved map report 78
saved scan report 40
scan dead hosts 101
scan functions
asset_domain.php 120
asset_group_list.php 132
asset_group.php 124
asset_ip_list.php 118
asset_ip.php 112
knowledgebase_download.php 49
overview 10, 22
scan_cancel.php 36
scan_options.php 100
scan_report_delete.php 42
scan_report_list.php 38
scan_report.php 40
scan_running_list.php 35
scan_target_history.php 44
scan.php 27
scheduled_scans.php 86
summary of functions 25
scan options
bandwidth impact 100
load balancer check 101
scan dead hosts 101
scan ports 102
scan options report
DTD 102, 271
XPath elements 272
scan ports 102
scan report
DTD 34, 41
scan report list 38
DTD 39, 225
XPath elements 226
scan request 27
scan summary notification 31
scan target 31, 32
scan target history 44
scan target history output
DTD 48, 231
XPath elements 232
scan_cancel.php function 36, 74
scan_options.php function 100
scan_report_delete.php function 42, 80
scan_report_list.php function 38
scan_report.php function 40
scan_running_list.php function 35, 73

scan_target_history.php function 44
scan.php function 27
scanner appliance 29, 32, 54, 62, 66, 71, 89, 103
scanner appliance list
DTD 273
XPath elements 273
scanner appliance, NAC option 274
scanner appliance, NAM option 274
scanner parallelization 24, 30, 32
scheduled scans
daily scans 91
list scheduled scans 97
monthly scans 92
remove scheduled scans 94
weekly scans 91
scheduled scans report
DTD 99, 262
XPath elements 99, 265
scheduled tasks report
DTD 99, 262
XPath elements 99, 265
scheduled_scans.php function 86
security audits 10, 21
special characters in URLs 15
state codes
Australia 190
Canada 190
India 190
United States of America 190

T

ticket delete output
DTD 162, 334
XPath elements 335
ticket edit output
DTD 160, 329
XPath elements 330
ticket functions 150
ticket information report
DTD 168, 341
XPath elements 345
ticket list deleted output
DTD 165, 338
XPath elements 339
ticket list output
DTD 157, 316
XPath elements 320
ticket state/status 154
ticket_delete.php function 161
ticket_edit.php function 158
ticket_list_deleted.php function 163
ticket_list.php function 155
time zone code list 96
time zone code list DTD 269
time_zone_code_list.php function 95
tracking method 111, 112

U

URL elements 15
URL encoded variables 15
user account
login credentials 13
user list output
DTD 200, 370
XPath elements 371
user management functions
acceptEULA.php 194
action_log_report.php 201
password_change.php 204
summary of functions 181
user_list.php 198
user.php 182, 196
user output
DTD 192, 197, 368
XPath elements 369
user_list.php function 198
user.php function 182, 196
country codes 189
state codes 190
UTF-8 encoding 15